(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 11 2005 001 672 T5** 2007.05.31

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2006/023151**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2005 001 672.2**
(86) PCT-Aktenzeichen: **PCT/US2005/024374**
(86) PCT-Anmeldetag: **08.07.2005**
(87) PCT-Veröffentlichungstag: **02.03.2006**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **31.05.2007**

(51) Int Cl.[8]: ***H04L 9/08*** (2006.01)

(30) Unionspriorität:
10/892,256 **14.07.2004** **US**

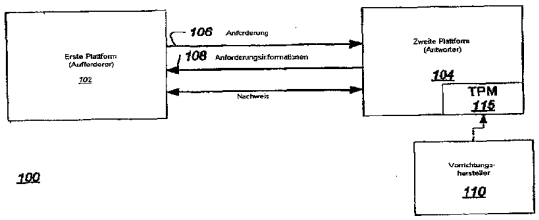
(71) Anmelder:
Intel Corp., Santa Clara, Calif., US

(74) Vertreter:
BOEHMERT & BOEHMERT, 28209 Bremen

(72) Erfinder:
Sutton, James, Portland, Oreg., US; Brickell, Ernest, Portland, Oreg., US; Hall, Clifford, Orangevale, Calif., US; Grawrock, David, Aloha, Oreg., US

(54) Bezeichnung: **Verfahren zum Liefern eines geheimen Direktnachweisschlüssels an Vorrichtungen unter Verwendung eines Onlinedienstes**

(57) Hauptanspruch: Verfahren umfassend:
Herstellen eines geschützten Onlineservers zur Unterstützung von Schlüsselabrufanfragen von Clientcomputersystemen;
Erzeugen eines Schlüsseldienst-Schlüsselpaars aus öffentlichem/geheimem Schlüssel in einer sicheren Schlüsselabrufverarbeitung;
Erzeugen eines pseudozufälligen Werts für eine Vorrichtung;
Erzeugen einer der Vorrichtung zugeordneten verschlüsselten Datenstruktur, wobei die verschlüsselte Datenstruktur einen geheimen Schlüssel umfaßt;
Erzeugen einer Kennung für die verschlüsselte Datenstruktur basierend auf dem pseudozufälligen Wert;
Speichern der Kennung und der verschlüsselten Datenstruktur auf dem geschützten Onlineserver; und
Speichern des pseudozufälligen Werts und eines Hash-Werts des öffentlichen Schlüssels des Schlüsseldiensts in einen nicht-flüchtigen Speicher in der Vorrichtung.



Beschreibung

1. GEBIET

[0001] Die vorliegende Erfindung betrifft allgemein Computersicherheit und insbesondere das sichere Verteilen kryptographischer Schlüssel an Vorrichtungen in Verarbeitungssystemen.

2. BESCHREIBUNG

[0002] Einige den Schutz von Inhalt und/oder Computersicherheitsmerkmale unterstützende Verarbeitungssystemstrukturen erfordern, daß speziell geschützte oder „gesicherte" Softwaremodule in der Lage sind, eine authentifizierte verschlüsselte Kommunikationssitzung mit spezifisch geschützten oder „gesicherten" Hardwarevorrichtungen in dem Verarbeitungssystem (wie zum Beispiel Graphiksteuerkarten) zu erzeugen. Ein zum Identifizieren der Vorrichtung und gleichzeitigem Erstellen der verschlüsselten Kommunikationssitzung allgemein verwendetes Verfahren ist die Verwendung eines einseitigen authentifizierten Diffie-Helman-(DH)-Schlüsselaustauschprozesses. Bei diesem Prozess wird der Vorrichtung ein eindeutiges Schlüsselpaar aus öffentlichem/geheimem Schlüssel nach dem Rivest/Shamir/Adelman-(RSA)-Algorithmus oder ein eindeutiges Schlüsselpaar nach der Elliptischen-Kurve-Kryptographie (ECC) zugewiesen. Da dieser Authentifizierungsprozess jedoch RSA- oder ECC-Schlüssel verwendet, weist die Vorrichtung dann eine eindeutige und nachweisbare Identität auf, was zu Datenschutzbedenken führen kann. Im schlimmsten Fall führen diese Bedenken zu einer mangelnden Unterstützung von Seiten der Hersteller von Originalgeräten bzw. Erstausrüster (Original Equipment Manufacturers = OEMs) beim Herstellen gesicherter Vorrichtungen, die diese Art von Sicherheit bereitstellen.

[0003] Die Vorteile und Merkmale der vorliegenden Erfindung werden aus der folgenden ausführlichen Beschreibung der Erfindung ersichtlich werden, in der:

[0004] Fig. 1 ein System veranschaulicht, das eine gemäß einem Trusted Platform Module (TPM) implementierte Plattform aufweist, die in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung betrieben wird;

[0005] Fig. 2 eine erste Ausführungsform der Plattform, die das TPM aus Fig. 1 enthält, veranschaulicht;

[0006] Fig. 3 eine zweite Ausführungsform der Plattform, die das TPM aus Fig. 1 enthält, veranschaulicht;

[0007] Fig. 4 eine beispielhafte Ausführungsform eines Computersystems veranschaulicht, das mit dem TPM aus Fig. 2 implementiert ist;

[0008] Fig. 5 ein Diagramm eines Systems zum Verteilen von Direktnachweisschlüsseln an Vorrichtungen unter Verwendung eines Onlinedienstes gemäß einer Ausführungsform der vorliegenden Erfindung ist;

[0009] Fig. 6 ein Flußdiagramm ist, das Stufen eines Verfahrens zum Verteilen von Direktnachweisschlüsseln unter Verwendung eines Onlinedienstes gemäß einer Ausführungsform der vorliegenden Erfindung verwendet;

[0010] Fig. 7 ist ein Flußdiagramm, das die Serveraufbauverarbeitung eines geschützten Servers gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0011] Fig. 8 ist ein Flußdiagramm, das die Aufbauverarbeitung von Vorrichtungsherstellern gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0012] Fig. 9 ist ein Flußdiagramm, das Herstellerproduktionsverarbeitung von Vorrichtungsherstellern gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht;

[0013] Fig. 10-Fig. 12 sind Flußdiagramme der Aufbauverarbeitung von Clientcomputersystemen gemäß einer Ausführungsform der vorliegenden Erfindung; und

[0014] Fig. 13 ist ein Flußdiagramm der Verarbeitung des Clientcomputersystems gemäß einer Ausführungsform der vorliegenden Erfindung.

AUSFÜHRLICHE BESCHREIBUNG

[0015] Die Verwendung des auf Direktnachweis basierenden Schlüsselaustauschprotokolls nach Diffie-Helman, um geschützten/gesicherten Vorrichtungen zu gestatten, sich selbst zu authentifizieren und eine verschlüsselte Kommunikationssitzung mit gesicherten Softwaremodulen herzustellen, vermeidet das Erzeugen jeder eindeutigen Identitätsinformation in dem Verarbeitungssystem und vermeidet dadurch das Einführen von Datenschutzbedenken. Das direkte Einbetten eines geheimen Direktnachweisschlüssels in eine Vorrichtung in einer Herstellungsanlage erfordert jedoch mehr geschützten nicht-flüchtigen Speicher in der Vorrichtung als andere Ansätze, wodurch die Kosten der Vorrichtung steigen. Eine Ausführungsform der vorliegenden Erfindung ist ein Verfahren, das es ermöglicht, den geheimen Direktnachweis-(DP)-Schlüssel (der z.B. zum Unterzeichnen verwendet wird) auf sichere Weise unter Verwendung eines Onlinedienstes an die Vorrichtung zu liefern

und danach durch die Vorrichtung selbst in der Vorrichtung zu installieren. Das in dieser Erfindung vorgestellte Verfahren ist so ausgelegt, daß die Vorrichtung für den Installationsprozess keine Identitätsinformationen offenlegen muß. In einer Ausführungsform kann die Verringerung des zur Unterstützung dieser Fähigkeit erforderlichen Vorrichtungsspeichers von etwa 300 bis 700 Bytes bis hinab auf etwa 40 Bytes betragen. Diese Verringerung der Menge nicht-flüchtigen Speichers, die zur Implementation des auf Direktnachweis basierenden Diffie-Helman-Schlüsselaustauschs erforderlich ist, kann zu einer breiteren Akzeptanz dieser Technik führen.

[0016] In Ausführungsformen der vorliegenden Erfindung werden geheime DP-Unterzeichnungsschlüssel nicht in oder mit einer Vorrichtung verteilt. Statt dessen unterstützt die Vorrichtung ein Protokoll, durch das die Vorrichtung in dem Gebiet ihren eigenen geheimen Schlüssel von einem durch einen Hersteller oder Anbieter oder einen Vertreter bereitgestellten geschützten Onlineserver sicher abrufen kann. Dieses Protokoll schafft einen gesicherten Kanal zwischen der Vorrichtung und dem Server und erfordert kein Vertrauen in eine dazwischen geschaltete Software, einschließlich einer Software auf einem lokalen Verarbeitungssystem.

[0017] Die Bezugnahme auf „eine Ausführungsform" in der Beschreibung bedeutet, daß ein bestimmtes Merkmal, eine bestimmte Struktur oder eine bestimmte Eigenschaft, die in Verbindung mit der Ausführungsform beschrieben werden, in mindestens einer Ausführungsform der vorliegenden Erfindung enthalten ist. Somit bezieht sich nicht jedes Auftreten der Formulierung „in einer Ausführungsform" an verschiedenen Stellen in der gesamten Beschreibung notwendigerweise auf dieselbe Ausführungsform.

[0018] In der folgenden Beschreibung wird eine bestimmte Terminologie zur Beschreibung bestimmter Merkmale einer oder mehrerer Ausführungsformen der Erfindung verwendet. Beispielsweise ist „Plattform" als jede Art von Kommunikationsvorrichtung definiert, die dazu ausgelegt ist, Informationen zu senden und zu empfangen. Zu Beispielen verschiedener Plattformen gehören, sind jedoch nicht darauf beschränkt oder eingeschränkt, Computersysteme, Personal Digital Assistants bzw. Minicomputer, Mobiltelefone, Set-Top-Boxen bzw. Digitalempfänger, Faxmaschinen, Drucker, Modems, Router oder dergleichen. Eine „Kommunikationsstrecke" ist allgemein definiert als ein oder mehrere Informationen tragende/s Medium bzw. Medien, die an eine Plattform angepasst sind. Zu Beispielen verschiedener Arten von Kommunikationsstrecken gehören, sind jedoch nicht darauf beschränkt oder eingeschränkt, elektrische Leitung(en), optische Faser(n), Kabel, Busleitung(en) oder drahtlose Signalgebungstechnologie.

[0019] Ein „Aufforderer" bezieht sich auf jede Einheit (z.B. Person, Plattform, System, Software und/oder Vorrichtung), die eine Verifizierung der Authentifikation oder Befugnis von einer anderen Einheit anfordert. Normalerweise erfolgt dies vor der Offenbarung oder Bereitstellung der angeforderten Informationen. Ein „Antworter" bezieht sich auf jede Einheit, die aufgefordert wurde, einen Nachweis über ihre Authentifizierung, Gültigkeit und/oder Identität bereitzustellen. Ein „Vorrichtungshersteller", was austauschbar mit „zertifizierender Hersteller" verwendet werden kann, bezieht sich auf jede Einheit, die eine Plattform oder eine Vorrichtung herstellt oder konfiguriert.

[0020] Gegenüber einem Aufforderer „nachzuweisen" oder ihn zu „überzeugen", daß ein Antworter im Besitz oder in Kenntnis kryptographischer Informationen ist (z.B. digitaler Unterschrift, ein Geheimnis wie ein geheimer Schlüssel usw.), bedeutet wie hierin verwendet, daß basierend auf der dem Aufforderer offenbarten Information und des dem Aufforderer offenbarten Nachweises eine große Wahrscheinlichkeit besteht, daß der Antworter über die kryptographische Information verfügt. Um dies einem Aufforderer gegenüber nachzuweisen, ohne die kryptographische Informationen „offenzulegen" oder „zu offenbaren", bedeutet, daß es, basierend auf der dem Aufforderer offenbarten Informationen, dem Aufforderer rechnungstechnisch unmöglich wäre, die kryptographische Information zu bestimmen.

[0021] Derartige Nachweise werden im folgenden als Direktnachweise bezeichnet. Der Ausdruck „Direktnachweis" bezieht sich auf Null-Kenntnis-Nachweise, wie diese Art von Nachweisen in dem Gebiet allgemein bekannt ist. Insbesondere ist ein spezifisches Direktnachweisprotokoll, wie das hierin erwähnte, der Gegenstand der gleichzeitig anhängigen Patentanmeldung Nr. 10/306,336, die am 27.11.2002 unter dem Titel „System and Method for Establishing Trust Without Revealing Identity" eingereicht und dem Inhaber der vorliegenden Anmeldung zugewiesen wurde. Direktnachweis definiert ein Protokoll, in dem ein Ausgeber eine Familie mit vielen Mitgliedern definiert, denen dieselben durch den Ausgeber definierten Eigenschaften gemein sind. Der Ausgeber erzeugt ein Schlüsselpaar öffentlichem/geheimem Schlüssel der Familie (Fpub und Fpri), das die Familie als Ganzes darstellt. Unter Verwendung von Fpri kann der Ausgeber auch einen eindeutigen geheimen Direktnachweisunterzeichnungsschlüssel (DPpri) für jedes einzelne Mitglied der Familie ausgeben. Jede durch einen einzelnen DPpri unterzeichnete Nachricht kann unter Verwendung des öffentlichen Schlüssels der Familie Fpub verifiziert werden. Eine solche Verifizierung identifiziert jedoch nur, daß der Unterzeichner ein Mitglied der Familie ist; es wird keine eindeutig identifizierende Information über das einzelne Mitglied offengelegt. In einer Ausführungs-

form kann der Ausgeber ein Vorrichtungshersteller oder ein Vertreter sein. Das heißt, bei dem Ausgeber kann es sich um eine Einheit mit der Fähigkeit handeln, basierend auf gemeinsamen Merkmalen Vorrichtungsfamilien zu definieren, das Schlüsselpaar aus öffentlichem geheimem Schlüssel zu erzeugen und geheime Direktnachweisschlüssel zu erstellen und in die Vorrichtung einzusetzen. Der Ausgeber kann auch Zertifikate für den öffentlichen Schlüssel der Familie erzeugen, die die Quelle des Schlüssels und die Eigenschaften der Vorrichtungsfamilie identifizieren.

[0022] Unter Bezugnahme nun auf Fig. 1 wird eine Ausführungsform eines Systems gezeigt, das eine mit einer gesicherten Hardwarevorrichtung implementierte Plattform (als „Trusted Platform Module" oder „TPM" bezeichnet) aufweist, die in Übereinstimmung mit einer Ausführungsform der Erfindung betrieben wird. Eine erste Plattform **102** (Aufforderer) sendet eine Anforderung **106**, daß eine zweite Plattform **104** (Antworter) Informationen über sich selbst bereitstellt. In Beantwortung der Anforderung **106** stellt die zweite Plattform **104** die angeforderten Informationen **108** bereit.

[0023] Zur Erhöhung der Sicherheit kann es zusätzlich erforderlich sein, daß die erste Plattform **102** verifizieren muß, das die angeforderte Information **108** von einer durch einen ausgewählten Vorrichtungshersteller oder eine ausgewählte Gruppe von Vorrichtungsherstellern (im folgenden „Vorrichtungshersteller **110**" genannt) hergestellten Vorrichtung kam. In einer Ausführungsform der Erfindung fordert die erste Plattform **102** beispielsweise die zweite Plattform **104**, auf zu zeigen, daß sie über kryptographische Informationen (z.B. eine Unterschrift) verfügt, welche durch den/die Vorrichtungshersteller **110** erzeugt worden sind. Die Aufforderung kann entweder in der Anforderung **106** (wie gezeigt) enthalten oder eine separate Sendung sein. Die zweite Plattform **104** antwortet auf die Aufforderung durch Bereitstellen von Informationen in Form einer Antwort, um die erste Plattform **102** zu überzeugen, daß die zweite Plattform **104** über kryptographische Informationen verfügt, die durch den/die Vorrichtungshersteller **110** erzeugt wurden, ohne die kryptographischen Informationen offenzulegen. Die Antwort kann entweder ein Teil der angeforderten Information **108** (wie gezeigt) oder eine separate Sendung sein.

[0024] In einer Ausführungsform der Erfindung umfaßt die zweite Plattform **104** ein Trusted Platform Module (TPM) **115**. Bei dem TPM **115** handelt es sich um eine von dem/den Vorrichtungshersteller/n **110** hergestellte kryptographische Vorrichtung. In einer Ausführungsform der Erfindung umfaßt das TPM **115** einen Prozessor mit einer geringen Menge von in einem Paket eingekapseltem On-Chip- bzw. chipinternen Speicher. Das TPM **115** ist so konfiguriert, daß es der ersten Plattform **102** Informationen bereitstellt, die sie dazu befähigen würden, zu bestimmen, daß eine Antwort von einem gültigen TPM gesendet wurde. Die verwendeten Informationen sind Inhalt, der es nicht wahrscheinlich machen würde, daß die Identität des TPM oder der zweiten Plattform bestimmt werden kann.

[0025] Fig. 2 veranschaulicht eine erste Ausführungsform der zweiten Plattform **104** mit dem TPM **115**. Bei dieser Ausführungsform der Erfindung umfaßt die zweite Plattform **104** einen mit dem TPM **115** gekoppelten Prozessor **202**. Im allgemeinen handelt es sich bei dem Prozessor **202** um eine Vorrichtung, die Informationen verarbeitet. In einer Ausführungsform der Erfindung kann der Prozessor beispielsweise als Mikroprozessor, Digitalsignalprozessor, Mikrosteuerung oder auch in einer Zustandsmaschine implementiert sein. Alternativ kann der Prozessor **202** in einer anderen Ausführungsform der Erfindung als programmierbare oder festcodierte Logik, wie feldprogrammierbare Gatearrays (FPGAs), Transistor-Transistor-Logik (TTL) oder auch anwendungsspezifische integrierte Schaltung (ASIC) implementiert sein.

[0026] Hier umfaßt die zweite Plattform **104** ferner eine Speichereinheit **206**, um die Speicherung kryptographischer Information, wie eine oder mehrere der folgenden zu gestatten: Schlüssel, Hash-Werte, Signaturen, Zertifikate usw. Ein Hash-Wert von „X" kann als „Hash(X)" dargestellt werden. Es wird in Betracht gezogen, daß solche Informationen in dem internen Speicher **220** des TPM **115** anstelle der Speichereinheit **206** wie in Fig. 3 gezeigt gespeichert werden. Die kryptographischen Informationen können verschlüsselt werden, insbesondere, wenn sie außerhalb des TPM **115** gespeichert werden.

[0027] Fig. 4 veranschaulicht eine Ausführungsform einer Plattform, die ein mit dem TPM **115** aus Fig. 2 implementiertes Computersystem **300** enthält. Das Computersystem **300** umfaßt einen Bus **302** und einen mit dem Bus **302** gekoppelten Prozessor **310**. Das Computersystem **300** umfaßt ferner eine Hauptspeichereinheit **304** und eine statische Speichereinheit **306**.

[0028] Bei der Hauptspeichereinheit **304** handelt es sich hier um einen flüchtigen Halbleiterspeicher zum Speichern von Informationen und durch Prozessor **310** ausgeführten Anweisungen. Der Hauptspeicher **304** kann auch zum Speichern temporärer Variablen oder anderer Zwischeninformationen während der Ausführung von Anweisungen durch den Prozessor **310** verwendet werden. Bei der statischen Speichereinheit **306** handelt es sich um einen nicht-flüchtigen Halbleiterspeicher zum Speichern von Informationen und Anweisungen für den Prozessor **310** auf einer permanenteren Basis. Zu Beispielen des statischen

Speichers **306** gehören, sind jedoch nicht darauf beschränkt oder eingeschränkt, Direktzugriffsspeicher (ROM). Sowohl die Hauptspeichereinheit **304** als auch die statische Speichereinheit **306** sind an den Bus **302** gekoppelt.

[0029] In einer Ausführungsform der Erfindung umfaßt das Computersystem **300** ferner eine Datenspeichervorrichtung **308** wie eine magnetische Disk bzw. Platte oder eine optische Disk bzw. Platte und ihr entsprechender Antrieb kann auch mit dem Computersystem **300** gekoppelt sein, um Informationen und Anweisungen zu speichern.

[0030] Das Computersystem **300** kann auch über den Bus **302** an eine Graphiksteuervorrichtung **314** gekoppelt sein, die eine (nicht gezeigte) Anzeige, wie eine Kathodenstrahlröhre (CRT), eine LCD-(Liquid Crystal Display)-Anzeige oder jede flache Tafelanzeige, steuert, um einem Endnutzer Informationen anzuzeigen. In einer Ausführungsform kann erwünscht sein, daß die Graphiksteuervorrichtung in der Lage ist, eine authentifizierte verschlüsselte Kommunikationssitzung mit einem durch den Prozessor ausgeführten Softwaremodul aufzubauen.

[0031] Typischerweise kann eine alphanumerische Eingabevorrichtung **316** (z.B. Tastatur, Tastenfeld usw.) an den Bus **302** zum Kommunizieren von Informationen und/oder Befehlsauswahl an den Prozessor **310** gekoppelt sein. Eine andere Art von Nutzereingabevorrichtung ist eine Cursorsteuereinheit **318**, wie eine Maus, ein Trackball, ein Touchpad, ein Stift oder Cursorrichtungstasten zum Kommunizieren von Richtungsinformationen und Befehlsauswahl an den Prozessor **310** und zum Steuern von Cursorbewegung auf der Anzeige **314**.

[0032] Eine Kommunikationsschnittstelleneinheit **320** ist ebenfalls an den Bus **302** gekoppelt. Zu Beispielen der Schnittstelleneinheit **320** gehören ein Modem, eine Netzwerkschnittstellenkarte oder andere wohlbekannte Schnittstellen, die zum Koppeln mit einer einen Teil eines lokalen oder breiten Gebietsnetzwerks bildenden Kommunikationsverbindung verwendet werden. Auf diese Weise kann das Computersystem **300** mit einer Anzahl von Clients und/oder Servern über eine herkömmliche Netzwerkinfrastruktur, wie zum Beispiel ein Intranet einer Firma und/oder dem Internet, gekoppelt werden. In einer Ausführungsform kann das Computersystem über ein Netzwerk oder einen geschützten Server online gekoppelt werden.

[0033] Es versteht sich, daß ein weniger oder mehr ausgestattetes Computersystem als oben beschrieben für bestimmte Implementationen wünschenswert sein kann. Daher wird die Konfiguration des Computersystems **300** von Implementation zu Implementation abhängig von zahlreichen Faktoren, wie Preisbeschränkungen, Leistungsanforderungen, technologischen Verbesserungen und/oder anderen Umständen variieren.

[0034] In mindestens einer Ausführungsform kann das Computersystem **300** die Verwendung von speziell geschützten „gesicherten" Softwaremodulen (z.B. manipulationsresistenter Software oder Systemen mit der Fähigkeit, geschützte Programme laufen zu lassen) unterstützen, die in dem Hauptspeicher **304** und/oder der Massenspeichervorrichtung **308** gespeichert und durch Prozessor **310** ausgeführt werden, um sogar in Gegenwart anderer feindlicher Software in dem System spezifische Tätigkeiten auszuführen. Einige dieser gesicherten Softwaremodule erfordern äquivalent „sicherbaren" geschützten Zugriff nicht nur auf andere Plattformen, sondern auf eine oder mehrere Peripherievorrichtungen innerhalb derselben Plattform, wie die Graphiksteuervorrichtung **314**. Im allgemeinen erfordert ein solcher Zugriff, daß das gesicherte Softwaremodul in der Lage ist, die Fähigkeiten und/oder die spezifische Identität der Vorrichtung zu identifizieren und dann eine verschlüsselte Sitzung mit der Vorrichtung einzurichten, um den Austausch von Daten zu gestatten, die von anderer Software in dem System nicht ausspioniert oder verfälscht werden können.

[0035] In einem Verfahren aus dem Stand der Technik zum Identifizieren der Vorrichtung und gleichzeitigem Einrichten der verschlüsselten Sitzung wird ein einseitiger authentifizierter Diffie-Heilman-(DH)-Schlüsselaustauschprozess verwendet. In diesem Prozess wird der Vorrichtung ein eindeutiges RSA- oder ECC-Schlüsselpaar aus öffentlichem und geheimen Schlüssel zugewiesen. Die Vorrichtung hält und schützt den geheimen Schlüssel, während der öffentliche Schlüssel zusammen mit Authentifikationszertifikaten an das Softwaremodul freigegeben werden kann. Während des DH-Schlüsselaustauschprozesses unterschreibt die Vorrichtung unter Verwendung ihres geheimen Schlüssels eine Nachricht, die von dem Softwaremodul unter Verwendung des entsprechenden öffentlichen Schlüssels verifiziert werden kann. Dies gestattet dem Softwaremodul die Authentifizierung, daß die Nachricht wirklich von der in Frage stehenden Vorrichtung kam.

[0036] Da dieser Authentifizierungsprozess jedoch RSA- oder ECC-Schlüssel verwendet, verfügt die Vorrichtung über eine eindeutige und nachweisbare Identität. Jedes Softwaremodul, das die Vorrichtung zum Unterzeichnen einer Nachricht mit ihrem geheimen Schlüssel bringen kann, kann nachweisen, daß diese spezifische eindeutige Vorrichtung in einem Computersystem vorhanden ist. Vor dem Hintergrund, daß Vorrichtungen selten zwischen Verarbeitungssystemen wandern, stellt dies auch eine nachweisbare eindeutige Computersystemidentität dar. Außerdem stellt der öffentliche Schlüssel der Vorrich-

tung selbst einen konstanten eindeutigen Wert, effektiv ein permanentes „Cookie" dar. In einigen Fällen können diese Merkmale als signifikantes Datenschutzproblem ausgelegt werden.

[0037] Ein alternativer Ansatz wird in der gleichzeitig anhängigen Patentanmeldung Nr. 10/???,???, die am ?/?/2004 unter dem Titel „An Apparatus and Method for Establishing an Authentificated Encrypted Session with a Device Without Exposing Privacy-Sensitive Information" eingereicht und an den Inhaber der vorliegenden Erfindung zugewiesen wurde, beschrieben. In diesem Ansatz wird die Verwendung von RSA- oder ECC-Schlüsseln in dem einseitigen authentifizierten Diffie-Helman-Prozess durch Direktnachweisschlüssel ersetzt. Eine diesen Ansatz verwendende Vorrichtung kann als zu einer spezifischen Vorrichtungsfamilie gehörig authentifiziert werden, zu der Bestätigungen über das Verhalten oder die Vertrauenswürdigkeit der Vorrichtung gehören können. Der Ansatz legt keine eindeutig identifizierenden Informationen offen, die zum Herstellen einer eindeutigen Identität, die das Verarbeitungssystem darstellt, verwendet werden könnten.

[0038] Obwohl dieser Ansatz gut funktioniert, erfordert er zusätzlichen Speicher in der Vorrichtung, um den geheimen Direktnachweisschlüssel zu halten, der größer als ein RSA- oder ECC-Schlüssel sein kann. Um die Lasten dieses zusätzlichen Speichererfordernisses abzumildern, definieren Ausführungsformen der vorliegenden Erfindung ein System und ein Prozess zum Sicherstellen, daß die Vorrichtung über den geheimen Direktnachweisschlüssel verfügt, wenn sie den Schlüssel benötigt, ohne daß wesentlicher zusätzlicher Speicher in der Vorrichtung erforderlich wäre.

[0039] In mindestens einer Ausführungsform der vorliegenden Erfindung speichert ein Vorrichtungshersteller eine pseudozufällige 128-Bit-Zahl in einer Vorrichtung in der Herstellungsanlage und ein viel größerer geheimer Direktnachweisschlüssel (DPpri) kann verschlüsselt und an die Vorrichtung in dem Gebiet unter Verwendung eines durch einen geschützten Server betriebenen Onlineservice geliefert werden. Andere Ausführungsformen können eine Nummer in die Vorrichtung speichern, die länger oder kürzer als 128 Bits ist. Dieser Prozess stellt sicher, daß nur eine bestimmte Vorrichtung ihren zugewiesenen DPpri-Schlüssel entschlüsseln und verwenden kann. Fig. 5 ist ein Diagramm eines Systems **500** zum Verteilen von Direktnachweisschlüsseln gemäß einer Ausführungsform der vorliegenden Erfindung. Es gibt vier Einheiten in dem System, ein geschütztes Vorrichtungsherstellungssystem **502**, ein Vorrichtungsherstellungsproduktionssystem **503**, ein Clientcomputersystem **504** und einen geschützten Server **522**. Das geschützte Vorrichtungsherstellungssystem umfaßt ein in dem Aufbau- bzw. Einrichtungsprozess vor der Herstellung einer Vorrichtung **506** verwendetes Verarbeitungssystem. Das geschützte Herstellungssystem **502** kann durch einen Vorrichtungshersteller so betrieben werden, daß das geschützte System vor Hackerangriffen außerhalb des Vorrichtungsherstellungsorts geschützt wird (es handelt sich z.B. um ein geschlossenes System). Das Herstellungsproduktionssystem **503** kann bei der Herstellung der Vorrichtungen verwendet werden. In einer Ausführungsform kann es sich bei dem geschützten System und dem Produktionssystem um dasselbe System handeln. Vorrichtung **506** umfaßt jede Hardwarevorrichtung zum Einschluss in das Clientcomputersystem (z.B. eine Speichersteuervorrichtung, eine Peripherievorrichtung wie eine Graphiksteuervorrichtung, eine E/A-Vorrichtung usw.). In Ausführungsformen der vorliegenden Erfindung umfaßt die Vorrichtung einen pseudozufälligen Wert RAND **508** und einen Hash-Wert **509** des öffentlichen Schlüssels des Schlüsseldiensts, der in dem nicht-flüchtigen Speicher der Vorrichtung gespeichert ist.

[0040] Das geschützte Herstellungssystem enthält eine geschützte Datenbank **510** und eine Erzeugungsfunktion **512**. Die geschützte Datenbank umfaßt eine Datenstruktur zum Speichern mehrerer pseudozufälliger Werte (mindestens einen pro herzustellender Vorrichtung), die durch die Erzeugungsfunktion **512** wie unten beschrieben erzeugt werden. Die Erzeugungsfunktion umfaßt Logik (software- oder hardwareimplementiert), um eine hierin Keyblob **514** genannte Datenstruktur zu erzeugen. Keyblob **514** umfaßt mindestens drei Einzeldaten. Ein geheimer Direktnachweisschlüssel (DPpri) umfaßt einen kryptographischen Schlüssel, der von einer Vorrichtung zum Unterzeichnen verwendet werden kann. Der Extrakt des geheimen Direktnachweisschlüssels **516** (DPpri Digest) umfaßt einen Nachrichtenextrakt des DPpri nach jedem wohlbekannten Verfahren zum Generieren eines sicheren Nachrichtenextrakts, wie SHA-1. Einige Ausführungsformen können einen pseudozufälligen Initialisierungsvektor (IV) **518** enthalten, der einen Bitstrom als Teil des Keyblob zu Kompatibilitätszwecken umfaßt. Wenn eine Stromchiffre für die Verschlüsselung verwendet wird, wird der IV in einem wohlbekannten Verfahren zum Verwenden eines IV in einer Stromchiffre verwendet. Wenn eine Blockchiffre für die Verschlüsselung verwendet wird, wird der IV als Teil der zu verschlüsselnden Nachricht verwendet, wodurch jedes Beispiel der Verschlüsselung verschieden wird. Das geschützte Herstellungssystem enthält auch einen öffentlichen Schlüssel des Schlüsseldienstes **507**, der für ein unten ausführlicher beschriebenes Onlineprotokoll verwendet wird.

[0041] In Ausführungsformen der vorliegenden Erfindung erzeugt das geschützte Herstellungssystem einen oder mehrere Keyblobs (wie unten ausführlicher beschrieben) und speichert die Keyblobs in ei-

ner Keyblobdatenbank **520** auf einem geschützten Server **522**. In einer Ausführungsform können sich viele Keyblobs in der Keyblobdatenbank befinden. Der geschützte Server kann durch den Vorrichtungshersteller, Vorrichtungsanbieter oder eine andere untergeordnete Einheit betrieben werden. Der geschützte Server kann unter Verwendung eines Netzwerks, wie beispielsweise des Internets, kommunikativ mit einem Clientcomputersystem **504** gekoppelt sein. Der geschützte Server enthält auch einen geheimen Schlüssel des Schlüsseldienstes **511** zur Verwendung in dem Onlineprotokoll zwischen dem geschützten Server und der Vorrichtung.

[0042] Ein Clientcomputersystem **504**, das ein Direktnachweisprotokoll zur Authentifizierung und zum Schlüsselaustausch einer Kommunikationssitzung mit einer in System **504** enthaltenen Vorrichtung **506** wünscht, kann einen ausgewählten Keyblob **514** aus der Keyblobdatenbank **520** auf dem geschützten Server unter Verwendung eines Schlüsselpaars aus öffentlichem geheimem Schlüssel und des unten ausführlicher beschriebenen Onlineprotokolls lesen. Die Keyblobdaten können von der Vorrichtung verwendet werden, um einen lokalisierten Keyblob **524** (wie unten beschrieben) zur Verwendung beim Implementieren des Direktnachweisprotokolls zu erzeugen. Die Vorrichtungstreibersoftware **526** wird durch das Clientcomputersystem ausgeführt, um die Vorrichtung **506** zu initialisieren und zu steuern.

[0043] In Ausführungsformen der vorliegenden Erfindung kann es fünf getrennte Betriebsstufen geben. Fig. 6 ist ein Flußdiagramm **600**, das Stufen eines Verfahrens veranschaulicht, welches Direktnachweisschlüssel gemäß einer Ausführungsform der vorliegenden Erfindung verteilt. Gemäß den Ausführungsformen der vorliegenden Erfindung können in jeder Stufe bestimmte Aktionen ausgeführt werden. Bei dem Vorrichtungshersteller gibt es mindestens drei Stufen: die Aufbaustufe **601** des geschützten Servers, die Ausbaustufe **602** des Vorrichtungsherstellers, die Produktionsstufe **604** des Vorrichtungsherstellers. Die Auflaustufe des geschützten Servers wird hier mit Bezug auf die Fig. 7 beschrieben. Die Aufbaustufe des Vorrichtungsherstellers wird hier mit Bezug auf Fig. 8 beschrieben. Die Produktionsstufe des Vorrichtungsherstellers wird hier mit Bezug auf Fig. 9 beschrieben. An einer Verbraucherstelle, die über das Clientcomputersystem verfügt, gibt es mindestens zwei Stufen: die Aufbaustufe **606** des Clientcomputersystems und die Verwendungsstufe **608** des Clientcomputersystems. Die Aufbaustufe des Clientcomputersystems wird hier mit Bezug auf die Fig. 10-Fig. 12 beschrieben. Die Verwendungsstufe des Clientcomputersystems wird hier mit Bezug auf Fig. 13 beschrieben.

[0044] Fig. 7 ist ein Flußdiagramm **700**, das die Ausbaustufenverarbeitung des geschützten Servers gemäß einer Ausführungsform der vorliegenden Erfindung veranschaulicht. Diese Verarbeitung kann vor der Herstellung von Vorrichtungen durch einen Vorrichtungshersteller ausgeführt werden. Bei Block **702** erzeugt ein Vorrichtungshersteller einen geschützten Server **522**, um Schlüsselabrufanforderungen zu unterstützen. In einer Ausführungsform ist der geschützte Server auf wohlbekannte Art kommunikativ mit dem Internet verbunden. Für verbesserte Sicherheit sollte es sich bei dem geschützten Server nicht um dasselbe Verarbeitungssystem handeln wie das geschützte Herstellungssystem oder das Herstellungsproduktionssystem. Bei Block **704** erzeugt der Vorrichtungshersteller ein Schlüsseldienst-Schlüsselpaar aus öffentlichem/geheimem Schlüssel, das für den durch den geschützten Server bereitgestellten Schlüsselabrufdienst verwendet werden wird. In einer Ausführungsform kann das Schlüsseldienst-Schlüsselpaar aus öffentlichem geheimem Schlüssel in dem geschützten Server gespeichert werden. Dieses Schlüsselpaar kann einmal für alle durch das System durchgeführte Verarbeitung gespeichert werden, oder ein neues Paar kann für jede Klasse von Vorrichtungen erzeugt werden. Bei Block **706** liefert der Vorrichtungshersteller den öffentlichen Schlüssel **507** des Schlüsseldienstes an das geschützte Herstellungssystem **502**.

[0045] Fig. 8 ist ein Flußdiagramm **800**, das die Aufbauverarbeitung der Vorrichtungsherstellung gemäß einer Ausführungsform der vorliegenden Erfindung zeigt. In einer Ausführungsform kann ein Vorrichtungshersteller diese Aktionen unter Verwendung eines geschützten Herstellungssystems **502** ausführen. Bei Block **802** erzeugt der Vorrichtungshersteller ein Schlüsselpaar der Direktnachweisfamilie (Fpub und Fpri) für jede herzustellende Vorrichtungsklasse. Jede einzige Vorrichtung wird über einen DPpri-Schlüssel verfügen, so daß eine unter Verwendung des DPpri erzeugte Unterschrift durch Fpub verifiziert werden kann. Eine Vorrichtungsklasse kann jede Gruppe oder Untergruppe von Vorrichtungen umfassen, wie beispielsweise eine ausgewählte Produktreihe (d.h. Art von Vorrichtung) oder Untergruppen eines Produkts basierend auf Versionsnummer oder anderen Merkmalen der Vorrichtungen. Das Schlüsselpaar der Familie ist für die Verwendung durch die Vorrichtungsklasse bestimmt, für die es erzeugt wurde.

[0046] Für jede herzustellende Vorrichtung führt die Erzeugungsfunktion **512** des geschützten Herstellungssystems **502** Blöcke **804** bis **820** aus. Zunächst erzeugt bei Block **804** die Erzeugungsfunktion einen eindeutigen pseudozufälligen Wert (RAND) **508**. In einer Ausführungsform beträgt die Länge von RAND **128** Bits. In anderen Ausführungsformen können andere Werte verwendet werden. In einer Ausführungsform können die pseudozufälligen Werte für eine Anzahl von Vorrichtungen im Voraus erzeugt werden.

Bei Block **806** erzeugt die Erzeugungsfunktion unter Verwendung einer Einwegfunktion f, die durch die Vorrichtung unterstützt wird, einen symmetrischen Verschlüsselungsschlüssel SKEY aus dem eindeutigen RAND-Wert (SKEY = f(RAND)). Bei der Einwegfunktion kann es sich um jeden bekannten Algorithmus handeln, der sich für diesen Zweck eignet (z.B. SHA-1, MGF1, Datenverschlüsselungsstandard (DES), Dreifach-DES, Fortgeschrittener Verschlüsselungsstandard (AES) usw.). Bei Block **808** erzeugt die Erzeugungsfunktion in einer Ausführungsform ein Kennungs-(ID)-Etikett, welches dafür verwendet werden wird, um auf den Keyblob **514** dieser Vorrichtung in der Keyblobdatenbank **520** auf dem geschützten Server **522** zu verweisen, indem SKEY verwendet wird, um einen „Nulleintrag" (z.B. eine geringe Anzahl von Nullbytes) (Vorrichtungs-Kennung = Verschlüsselung (0..0) unter Verwendung von SKEY) zu verschlüsseln. In anderen Ausführungsformen können andere Arten der Erzeugung der Vorrichtungs-Kennung verwendet werden oder andere Werte können durch SKEY verschlüsselt werden.

[0047] Als nächstes erzeugt die Erzeugungsfunktion bei Block **810** den geheimen Direktnachweis-Unterzeichnungsschlüssel DPpri, der zu dem öffentlichen Schlüssel (Fpub) der Familie korreliert. Bei Block **812** hasht die Erzeugungsfunktion den DPpri, um unter Verwendung bekannter Verfahren den DPpri-Extrakt zu erzeugen (z.B. unter Verwendung von SHA-1 oder eines anderen Hash-Algorithmus). Bei Block **814** baut die Erzeugungsfunktion eine Keyblobdatenstruktur für die Vorrichtung auf. Der Keyblob enthält mindestens DPpri und den DPpri-Extrakt. In einer Ausführungsform enthält der Keyblob auch einen zufälligen Initialisierungsvektor mit einer Vielzahl pseudozufällig erzeugter Bits. Diese Werte können unter Verwendung von SKEY zum Erzeugen eines verschlüsselten Keyblob **514** verwendet werden. Bei Block **816** können die Vorrichtungs-Kennung, die bei Block **808** erzeugt wurde, und der bei Block **81** erzeugte verschlüsselte Keyblob **514** in einem Eintrag in einer Keyblobdatenbank **520** gespeichert werden. In einer Ausführungsform kann der Eintrag in der Keyblobdatenbank durch die Vorrichtungs-Kennung angezeigt werden. Bei Block **818** kann der aktuelle RAND-Wert in der geschützten Datenbank **510** gespeichert werden. Bei Block **820** können SKEY und DPpri gelöscht werden, da sie durch die Vorrichtung in dem Gebiet neu erzeugt werden.

[0048] Die Erzeugung des DPpri-Extrakts und die nachfolgende Verschlüsselung durch SKEY sind so aufgebaut, daß der Inhalt von DPpri nicht durch eine Einheit bestimmt werden kann, die nicht im Besitz von SKEY ist, und so, daß der Inhalt des KeyBlob durch eine Einheit, die nicht im Besitz von SKEY ist, ohne nachfolgende Detektion durch eine Einheit, die im Besitz von SKEY ist, nicht modifiziert werden kann. In anderen Ausführungsformen können andere Verfahren zum Bereitstellen dieses Geheim- und Integritätsschutzes verwendet werden. In einigen Ausführungsformen kann der Integritätsschutz nicht erforderlich sein und es könnte ein Verfahren verwendet werden, das nur Geheimheit bereitstellt. In diesem Fall wäre der Wert des DPpri-Extrakts nicht notwendig.

[0049] Zu einer beliebigen Zeit nach Block **820** kann bei Block **822** die geschützte Datenbank der RAND-Werte sicher auf das Herstellungsproduktionssystem **503** hochgeladen werden, das die RAND-Werte während der Herstellung in die Vorrichtungen speichert. Nach Verifizierung dieses Hochladens könnten die RAND-Werte sicher von dem geschützten Herstellungssystem **502** gelöscht werden. Bei Block **824** kann schließlich die Keyblobdatenbank **520** mit einer Vielzahl von verschlüsselten Keyblobs auf dem geschützten Server **522** gespeichert werden, wobei nur ein Keyblobdatenbankeintrag für jede Vorrichtung, wie durch das Vorrichtungs-Kennungs-Feld angezeigt, verwendet wird.

[0050] Fig. 9 ist ein Flußdiagramm **900**, das die Vorrichtungsherstellungsproduktionsverarbeitung nach einer Ausführungsform der vorliegenden Erfindung veranschaulicht. Wenn die Vorrichtungen in einer Produktionsanlage hergestellt werden, wählt das Herstellungsproduktionssystem bei Block **902** einen ungenutzten RAND-Wert von der geschützten Datenbank aus. Der ausgewählte RAND-Wert kann dann in nicht-flüchtigen Speicher in einer Vorrichtung gespeichert werden. In einer Ausführungsform umfaßt der nicht-flüchtige Speicher ein TPM. In einer Ausführungsform kann der RAND-Wert in ungefähr 16 Bytes nicht-flüchtigen Speichers gespeichert werden. Bei Block **904** kann ein Hash **509** des öffentlichen Schlüssels **507** des Schlüsseldiensts in dem nicht-flüchtigen Speicher der Vorrichtung gespeichert werden. Der Hash kann unter Verwendung eines bekannten Hash-Algorithmus erzeugt werden. In einer Ausführungsform kann der Hash-Wert in ungefähr 20 Bytes des nicht-flüchtigen Speichers gespeichert werden. Bei Block **906** zerstört das Herstellungsproduktionssystem, sobald die Speicherung des RAND-Werts erfolgreich war, jeden Nachweis über den RAND-Wert dieser Vorrichtung in der geschützten Datenbank **510**. An diesem Punkt ist das einzige Exemplar des RAND-Werts in der Vorrichtung gespeichert.

[0051] In einer alternativen Ausführungsform könnte der RAND-Wert während der Herstellung einer Vorrichtung erzeugt und dann an das geschützte Herstellungssystem zur Berechnung eines Keyblobs gesendet werden.

[0052] In einer weiteren Ausführungsform könnte der RAND-Wert an der Vorrichtung erzeugt werden und die Vorrichtung und das geschützte Herstel-

lungssystem könnten an einem Protokoll teilnehmen, um den DPpri-Schlüssel unter Verwendung eines Verfahrens zu erzeugen, das den DPpri-Schlüssel außerhalb der Vorrichtung nicht offenlegt. Die Vorrichtung kann dann die Vorrichtungs-Kennung, den SKEY und den Keyblob erzeugen. Die Vorrichtung würde die Vorrichtungs-Kennung und den Keyblob an das Herstellungssystem zum Speichern in der geschützten Datenbank **510** weitergeben. In diesem Verfahren bleiben dem Herstellungssystem dieselben Informationen (Vorrichtungs-Kennung, Keyblob) in der geschützten Datenbank, aber es kennt die Werte von RAND oder DPpri nicht.

[0053] Fig. 10-Fig. 12 sind Flußdiagramme der Aufbauverarbeitung des Clientcomputersystems gemäß einer Ausführungsform der vorliegenden Erfindung. Ein Clientcomputersystem kann diese Aktionen als Teil eines Hochfahrens des Systems ausführen. Beginnend bei Strom **1000** in Fig. 10 kann bei Block **1002** das Clientcomputersystem auf normale Weise hochgefahren werden und ein Vorrichtungstreiber-Softwaremodul **526** für die Vorrichtung kann in den Hauptspeicher des Clientcomputersystems geladen werden. Wenn der Vorrichtungstreiber initialisiert ist und mit der Ausführung beginnt, bestimmt der Vorrichtungstreiber bei Block **1004**, ob in der Massenspeichervorrichtung **308** für Vorrichtung **506** bereits ein verschlüsselter lokalisierter Keyblob **524** gespeichert ist. Wenn einer gespeichert ist, muß keine weitere Aufbauverarbeitung durchgeführt werden und die Aufbauverarbeitung endet bei Block **1006**. Wenn nicht, dann fährt die Verarbeitung mit Block **1008** fort. Bei Block **1008** gibt der Vorrichtungstreiber einen Befehl zum Erhalten des Schlüssels an die Vorrichtung **506** aus, um den Prozess zum Erhalt des geheimen Direktnachweisschlüssels zu initiieren.

[0054] Bei Block **1010** sendet der Vorrichtungstreiber den öffentlichen Schlüssel **507** des Schlüsseldiensts an die Vorrichtung. Bei Block **1014** extrahiert die Vorrichtung den öffentlichen Schlüssel des Schlüsseldiensts, erzeugt einen Hash-Wert des öffentlichen Schlüssels des Schlüsseldiensts und vergleicht den Hash-Wert des empfangenen öffentlichen Schlüssels des Schlüsseldienstes mit dem in dem nicht-flüchtigen Speicher der Vorrichtung gespeicherten Hash **509** des öffentlichen Schlüssels des Schlüsseldienst. Wenn die Hash-Werte übereinstimmen, ist von dem empfangenen öffentlichen Schlüssel des Schlüsseldienstes bekannt, dass er der des Schlüsselabrufdiensts des Vorrichtungsherstellers ist, und die Clientcomputersystemaufbauverarbeitung fährt fort.

[0055] In einer anderen Ausführungsform könnte die Vorrichtung ein Zertifikat eines zertifizierten öffentlichen Schlüssels des Schlüsseldienstes empfangen, für den das Zertifikat durch eine Zertifikatkette an den öffentlichen Schlüssel des Schlüsseldienstes verifiziert werden könnte, dessen Hash-Wert der in dem nicht-flüchtigen Speicher der Vorrichtung gespeicherte Hash-Wert **509** des öffentlichen Schlüssels des Schlüsseldiensts ist. Der zertifizierte öffentliche Schlüssel des Schlüsseldienstes könnte als der öffentliche Schlüssel des Schlüsseldienstes in den nachfolgenden Schritten verwendet werden.

[0056] Bei Block **1018** verwendet die Vorrichtung ihre Einwegfunktion f um den symmetrischen Schlüssel SKEY aus dem eingebetteten RAND-Wert **508** (SKEY = f(RAND)) wieder zu erstellen. Bei Block **1020** erzeugt die Vorrichtung dann ihr eindeutiges Vorrichtungs-ID-Etikett unter Verwendung des SKEY, um einen „Nulleintrag" (z.B. eine geringe Anzahl von Nullbytes) (Vorrichtungs-Kennung = Verschlüsselung (0..0) unter Verwendung von SKEY) zu verschlüsseln. Die Verarbeitung fährt mit Flußdiagramm **1100** von Fig. 11 fort.

[0057] Bei Block **1102** aus Fig. 11 erzeugt die Vorrichtung einen transienten symmetrischen Schlüssel Tkey. Dieser Schlüssel wird an den geschützten Server gesendet, der ihn zum Verschlüsseln der Nachricht verwenden kann, die der geschützte Server an die Vorrichtung zurückgibt. Bei Block **1104** baut die Vorrichtung eine Schlüsselabfrageanforderungsnachricht auf, die die Vorrichtungskennung und den transienten symmetrischen Schlüssel Tkey enthält,. verschlüsselt die Nachricht unter Verwendung des von dem Vorrichtungstreiber bei Block **1014** empfangenen öffentlichen Schlüssels des Schlüsseldienstes und sendet die Schlüsselabfrageanforderungsnachricht an den geschützten Server über den Vorrichtungstreiber. (Schlüsselabfrageanforderung = Verschlüsseln (Vorrichtungskennung, Tkey) mit dem öffentlichen Schlüssel des Schlüsseldienstes). Einem Fachmann wird ersichtlich sein, daß zur Verschlüsselung der Nachricht mit einem öffentlichen Schlüssel in der Regel ein Sitzungsschlüssel (Skey) für eine symmetrische Chiffre erzeugt werden würde, der Sitzungsschlüssel mit dem öffentlichen Schlüssel verschlüsselt werden würde und die Nachricht dann mit dem Sitzungsschlüssel verschlüsselt werden würde. Bei Block **1106** verschlüsselt der geschützte Server die empfangene Schlüsselabfragenachricht unter Verwendung des geheimen Schlüssels **511** des Schlüsseldienstes und extrahiert die darin gespeicherten Felder. Da der geschützte Server nun die Vorrichtungskennung kennt (die von der Schlüsselanforderungsnachricht erhalten wurde), sucht der geschützte Server in der Keyblobdatenbank nach dem Datensatz, der den passenden Vorrichtungkennungswert enthält und extrahiert den verschlüsselten Keyblob der Vorrichtung von dem Datensatz. Bei Block **1110** baut der geschützte Server eine zweite Antwortnachricht auf, die den öffentlichen Schlüssel der Familie und den verschlüsselten Keyblob enthält und verschlüsselt die zweite Antwortnachricht unter Verwendung des transienten symmetrischen Schlüs-

sels Tkey, der durch die Vorrichtung zugeführt wird. Somit ist die Schlüsselantwort = (öffentlicher Schlüssel der Familie, Verschlüsselung des (verschlüsselten Keyblobs) unter Verwendung von Tkey). Das Verschlüsseln des verschlüsselten Keyblob mit Tkey erfolgt nicht zum Schützen des Keyblob, da es bereits mit einem symmetrischen Schlüssel SKEY verschlüsselt ist, der nur durch die Vorrichtung wieder hergestellt werden kann. Vielmehr stellt das Verschlüsseln der Nachricht auf diese Weise sicher, dass sich der zurückgegebene Keyblob jedesmal beim Ausführen des Prozesses zum Erhalten des Schlüssels ändert, wodurch sichergestellt wird, dass der Keyblob selbst als ein „Cookie" verwendet werden kann. Die zweite Antwortnachricht kann an den Vorrichtungstreiber auf dem Clientcomputersystem bei Block **1112** zurückgegeben werden, welcher die Nachricht an die Vorrichtung weiterleitet.

[0058] Bei Block **1114** extrahiert die Vorrichtung den öffentlichen Schlüssel der Familie von der zweiten Antwortnachricht, entschlüsselt den verpackten Keyblob unter Verwendung des transienten symmetrischen Schlüssels Tkey und speichert den verschlüsselten Keyblob in dem flüchtigen Speicher der Vorrichtung. Die Verarbeitung fährt dann mit Flußdiagramm **1200** von Fig. 12 fort.

[0059] Bei Block **1216** von Fig. 12 entschlüsselt die Vorrichtung den verschlüsselten Keyblob unter Verwendung des symmetrischen Schlüssels SKEY, um DPpri und den DPpri-Extrakt zu ergeben und speichert diese Werte in seinem nicht-flüchtigen Speicher (Entschlüsselter Keyblob = Entschlüsseln (IV, DPpri, DPpri-Extrakt) unter Verwendung von SKEY). Der Initialisierungsvektor (IV) kann verworfen werden. Bei Block **1218** prüft die Vorrichtung dann die Integrität von DPpri durch Hashen von DPpri und Vergleichen des Ergebnisses mit dem DPpri-Extrakt. Wenn der Vergleich gut ist, nimmt die Vorrichtung DPpri als gültigen Schlüssel an. Die Vorrichtung kann in einer Ausführungsform auch eine Schlüssel-Erhalten-Fahne setzen, um anzuzeigen, dass der geheime Direktnachweisschlüssel erfolgreich erhalten wurde. Bei Block **1220** wählt die Vorrichtung einen neuen IV und erzeugt einen neuen verschlüsselten lokalisierten Keyblob unter Verwendung des neuen IV (Lokalisierter Keyblob = Verschlüsseln (IV2, DPpri, DPpri-Extrakt) unter Verwendung von SKEY). In einer Ausführungsform kann der neue verschlüsselte Keyblob an ein Schlüsselabrufeinheit-Softwaremodul (in Fig. 5 nicht gezeigt) auf dem Clientcomputersystem zurückgegeben werden. Bei Block **1222** speichert die Schlüssel-Abfrageeinheit den verschlüsselten lokalisierten Keyblob in dem Speicher des Clientcomputersystems (wie beispielsweise der Massenspeichervorrichtung **308**). Der DPpri der Vorrichtung ist nun sicher in das Clientcomputersystem gespeichert.

[0060] Sobald die Vorrichtung während der Aufbauverarbeitung den DPpri erhalten hat, kann die Vorrichtung dann den DPpri verwenden. Fig. 13 ist ein Flußdiagramm **1300** der Clientcomputersystemverarbeitung gemäß einer Ausführungsform der vorliegenden Erfindung. Das Clientcomputersystem kann diese Aktionen jederzeit ausführen, nachdem der Aufbau abgeschlossen ist. Bei Block **1302** kann das Clientcomputersystem auf normale Weise hochgefahren werden und ein Vorrichtungstreiber **526** für die Vorrichtung kann in den Hauptspeicher geladen werden. Wenn der Vorrichtungstreiber initialisiert wird und mit der Ausführung beginnt, bestimmt der Vorrichtungstreiber, ob in der Massenspeichervorrichtung **308** für die Vorrichtung **506** bereits ein verschlüsselter lokalisierter Keyblob **524** gespeichert ist. Wenn nicht, wird die Aufbauverarbeitung aus Fig. 10-Fig. 12 ausgeführt. Wenn für diese Vorrichtung ein verschlüsselter lokalisierter Keyblob verfügbar ist, fährt die Verarbeitung mit Block **1306** fort. Bei Block **1306** fragt der Vorrichtungstreiber den verschlüsselten lokalisierten Keyblob ab und überträgt den Keyblob an die Vorrichtung. In einer Ausführungsform kann die Übertragung des Keyblob durch Ausführen eines Keyblob-Lade-Befehls erfolgen.

[0061] Bei Block **1308** verwendet die Vorrichtung ihre Einwegfunktion f, um den symmetrischen Schlüssel SKEY (nun zur Verwendung in der Entschlüsselung) aus dem eingebetteten RAND-Wert **508** (SKEY = f(RAND)) wiederzugewinnen. Bei Block **1310** entschlüsselt die Vorrichtung den verschlüsselten lokalisierten Keyblob unter Verwendung des symmetrischen Schlüssels SKEY, um DPpri und DPpri-Extrakt zu ergeben, und speichert diese Werte in seinem nichtflüchtigen Speicher (entschlüsselter Keyblob = Entschlüsseln (IV2, DPpri, DPpri-Extrakt) unter Verwendung von SKEY). Der zweite Initialisierungsvektor (IV2) kann verworfen werden. Bei Block **1312** prüft die Vorrichtung die Integrität des DPpri durch Hashen des DPpri und Vergleichen des Ergebnisses mit dem DPpri-Extrakt. Wenn der Vergleich gut ist (z.B. wenn der Extrakt übereinstimmt), nimmt die Vorrichtung DPpri als den früher erhaltenen gültigen Schlüssel an und aktiviert ihn zum Gebrauch. Die Vorrichtung kann auch eine Schlüssel-Erhalten-Fahne setzen, um anzuzeigen, dass der geheime Direktnachweisschlüssel erfolgreich erhalten wurde. Bei Block **1314** wählt die Vorrichtung noch einen anderen IV und schafft einen neuen verschlüsselten lokalisierten Keyblob unter Verwendung des neuen IV (Lokalisierter Keyblob = Verschlüsseln (IV3, DPpri, DPpri-Extrakt) unter Verwendung von SKEY). Der neue verschlüsselte lokalisierte Keyblob kann an die Schlüsselabfrageeinheit zurückgegeben werden. Bei Block **1316** speichert die Schlüsselabfrageeinheit den verschlüsselten, lokalisierten Keyblob in dem Speicher in dem Clientcomputersystem (wie beispielsweise der Massenspeichervorrichtung **308**). Der DPpri der Vorrichtung wird nun noch einmal in dem Clientcomputersystem sicher gespeichert.

[0062] In einer Ausführungsform der vorliegenden Erfindung ist es nicht notwendig, alle geheimen Direktnachweisschlüssel der Vorrichtung zur selben Zeit zu erzeugen. Angenommen, dass die Keyblobdatenbank auf dem geschützten Server regelmäßig aktualisiert wird, könnten die geheimen Direktnachweisschlüssel der Vorrichtung nach Bedarf erzeugt werden. Bei jeder Aktualisierung der Keyblobdatenbank auf dem geschützten Server würde er die aktuell erzeugte Keyblobdatenbank enthalten, einschließlich jeder Vorrichtungsschlüssel, die erzeugt worden sind, aber noch keinen Vorrichtungen zugewiesen worden sind.

[0063] In einer weiteren Ausführungsform kann es möglich sein, die Erzeugung des DPpri-Schlüssels der Vorrichtung zu verzögern, wodurch ermöglicht wird, diese Schlüssel nur für die Vorrichtungen zu erzeugen, die sie benötigen. Nach Empfang der ersten Anforderung zum Erhalten des Schlüssels von der Vorrichtung kann der geschützte Server eine Anforderung an das geschützte Herstellungssystem erzeugen, das immer noch den RAND-Wert der Vorrichtung hält. Zu dieser Zeit erzeugt das geschützte Herstellungssystem den DPpri -Schlüssel für die Vorrichtung, gibt ihn an den geschützten Server zurück und zerstört den RAND-Wert erst dann.

[0064] In einer weiteren Ausführungsform kann der Vorrichtungshersteller, statt den Hash-Wert des öffentlichen Schlüssels des Schlüsseldienstes in nicht-flüchtigem Speicher an der Vorrichtung zu speichern, den Hash-Wert eines Wurzelschlüssels speichern und dann Zertifikate für öffentliche Schlüssel des Schlüsseldienstes mit dem Wurzelschlüssel unterzeichnen. Auf diese Weise könnte derselbe Wurzelschlüssel für eine sehr große Anzahl von Vorrichtungen verwendet werden.

[0065] Obwohl die hier erörterten Vorgänge als ein sequentieller Prozess beschrieben werden können, könnten einige der Vorgänge tatsächlich parallel oder gleichzeitig ausgeführt werden. Außerdem kann in einigen Ausführungsformen die Reihenfolge der Vorgänge neu angeordnet werden, ohne von der Idee der Erfindung abzuweichen.

[0066] Die hier beschriebenen Techniken sind nicht auf eine bestimmte Hardware- oder Softwarekonfiguration beschränkt, sie können in jeder Rechen- oder Verarbeitungsumgebung zur Anwendung gelangen. Die Techniken können in Hardware, Software oder einer Kombination der beiden implementiert werden. Die Techniken können in Programmen implementiert werden, die auf programmierbaren Maschinen laufen, wie mobilen oder stationären Computern, Personal Digital Assistants bzw. Minicomputer, Set-Top-Boxen bzw. Digitalempfängern, Mobiltelefonen und Pagern und anderen elektronischen Vorrichtungen, die jeweils einen Prozessor, ein durch den Prozessor lesbares Speichermedium (einschließlich nicht-flüchtigen Speichers und/oder Speicherelementen), mindestens eine Eingabevorrichtung und eine oder mehrere Ausgabevorrichtuncode angelegt, um die beschriebenen Funktionen auszuführen und Ausgabeinformationen zu erzeugen. Die Ausgabeinformationen können an eine oder mehrere Ausgabevorrichtungen angelegt werden. Einem Durchschnittsfachmann dürfte klar sein, dass die Erfindung mit verschiedenen Computersystemkonfigurationen, einschließlich Multiprozessorsystemen, Minicomputern, Mainframecomputern und der gleichen ausgeführt werden kann. Die Erfindung kann auch in verteilten Rechenumgebungen ausgeführt werden, in denen Aufgaben durch entfernte Verarbeitungsvorrichtungen, die über ein Kommunikationsnetzwerk verbunden sind, ausgeführt werden.

[0067] Jedes Programm kann in einer auf Abläufe oder Objekte ausgerichteten Programmiersprache hohen Niveaus implementiert sein, um mit einem Verarbeitungssystem zu kommunizieren. Wenn gewünscht, können Programme jedoch in Programmumwandlungs- oder Maschinensprache implementiert sein. In jedem Fall kann die Sprache kompiliert oder interpretiert bzw. übersetzt sein.

[0068] Programmanweisungen können verwendet werden, um ein Verarbeitungssystem für den allgemein oder speziellen Gebrauch zu erzeugen, das mit den Anweisungen programmiert wird, um die hier beschriebenen Vorgänge durchzuführen. Alternativ können die Vorgänge durch spezifische Hardwarekomponenten ausgeführt werden, die zum Ausführen der Vorgänge Hardwarelogik enthalten, oder durch eine beliebige Kombination programmierter Computerkomponenten und angepasster Hardwarekomponenten. Die hier beschriebenen Verfahren können als Computerprogrammprodukt bereitgestellt werden, das ein maschinenlesbares Medium enthalten kann, das darauf Anweisungen gespeichert haben kann, die verwendet werden können, um ein Verarbeitungssystem oder eine andere elektronische Vorrichtung zur Ausführung der Verfahren zu programmieren. Der Begriff „maschinenlesbares Medium" soll, wie hierin verwendet, jedes Medium einschließen, das in der Lage ist, eine Abfolge von Anweisungen zur Ausführung durch eine Maschine zu speichern oder zu codieren und das bewirkt, dass die Maschine eines der hier beschriebenen. Verfahren ausführt. Der Begriff „maschinenlesbares Medium" soll dementsprechend Festzustands- bzw. Halbleitermedien, optische und magnetische Disks und eine Trägerwelle, die ein Datensignal codiert, enthalten, aber nicht darauf beschränkt sein. Außerdem ist es in dem Gebiet üblich, in der einen oder anderen Form von Software so zu sprechen (z.B. Programm, Verfahren, Prozess, Anwendung, Modul, Logik und so weiter), dass sie eine Aktion vornimmt oder ein Ergebnis hervorruft. Derartige Ausdrücke sind lediglich die Kurz-

fassung, um die Ausführung der Software durch ein Verarbeitungssystem festzustellen, welche bewirkt, dass der Prozessor eine Aktion ausführt oder ein Ergebnis erzeugt.

[0069] Während die vorliegende Erfindung mit Bezug auf veranschaulichende Ausführungsformen beschrieben wurde, soll diese Beschreibung nicht in einem einschränkenden Sinn ausgelegt werden. Verschiedene Modifikationen der veranschaulichenden Ausführungsformen sowie andere Ausführungsformen der Erfindung, welche Fachleuten auf dem Gebiet, zu dem die Erfindung gehört, ersichtlich sind, sollen innerhalb der Idee und des Schutzumfangs der Erfindung liegen.

ZUSAMMENFASSUNG

[0070] Das Liefern eines geheimen Direktnachweisschlüssels an eine in einem Clientcomputersystem in dem Gebiet installierte Vorrichtung kann auf sichere Weise erzielt werden, ohne daß ein signifikanter nicht-flüchtiger Speicher in der Vorrichtung erforderlich ist. Bei der Herstellung wird ein eindeutiger pseudozufälliger Wert erzeugt und in der Vorrichtung gespeichert. Der pseudozufällige Wert wird verwendet, um einen symmetrischen Schlüssel zum Verschlüsseln einer Datenstruktur zu erzeugen, welche einen geheimen Direktnachweisschlüssel und einen der Vorrichtung zugeordneten Extrakt des geheimen Schlüssels enthält. Die sich ergebende verschlüsselte Datenstruktur wird in einem geschützten Onlineserver gespeichert, der durch das Clientcomputersystem zugänglich ist. Beim Initialisieren der Vorrichtung in dem Clientcomputersystem prüft das System, ob in dem System eine lokalisierte verschlüsselte Datenstruktur vorhanden ist. Wenn nicht, erhält das System die zugeordnete verschlüsselte Datenstruktur von dem geschützten Onlineserver unter Verwendung eines sicheren Protokolls. Die Vorrichtung entschlüsselt die verschlüsselte Datenstruktur unter Verwendung eines symmetrischen Schlüssels, der aus seinem gespeicherten pseudozufälligen Wert wiederhergestellt wurde, um einen geheimen Direktnachweisschlüssel zu erhalten. Wenn der geheime Schlüssel gültig ist, kann er für die nachfolgende Authentifizierungsverarbeitung durch die Vorrichtung in dem Clientcomputersystem verwendet werden.

Patentansprüche

1. Verfahren umfassend:
Herstellen eines geschützten Onlineservers zur Unterstützung von Schlüsselabrufanfragen von Clientcomputersystemen;
Erzeugen eines Schlüsseldienst-Schlüsselpaars aus öffentlichem/geheimem Schlüssel in einer sicheren Schlüsselabrufverarbeitung;
Erzeugen eines pseudozufälligen Werts für eine Vorrichtung;
Erzeugen einer der Vorrichtung zugeordneten verschlüsselten Datenstruktur, wobei die verschlüsselte Datenstruktur einen geheimen Schlüssel umfaßt;
Erzeugen einer Kennung für die verschlüsselte Datenstruktur basierend auf dem pseudozufälligen Wert;
Speichern der Kennung und der verschlüsselten Datenstruktur auf dem geschützten Onlineserver; und
Speichern des pseudozufälligen Werts und eines Hash-Werts des öffentlichen Schlüssels des Schlüsseldiensts in einen nicht-flüchtigen Speicher in der Vorrichtung.

2. Verfahren nach Anspruch 1, ferner umfassend ein Erzeugen eines Schlüsselpaars der Direktnachweisfamilie für eine Vorrichtungsklasse.

3. Verfahren nach Anspruch 2, wobei der geheime Schlüssel einen einem öffentlichen Schlüssel aus dem Schlüsselpaar der Direktnachweisfamilie zugeordneten geheimen Direktnachweisschlüssel umfaßt, und ferner umfassend ein Hashen des geheimen Direktnachweisschlüssels zum Erzeugen des Extrakts des geheimen Schlüssels.

4. Verfahren nach Anspruch 1, ferner umfassend ein Erzeugen eines symmetrischen Schlüssels basierend auf dem pseudozufälligen Wert für die Vorrichtung.

5. Verfahren nach Anspruch 4, wobei das Erzeugen der Kennung das Verschlüsseln eines Datenwerts unter Verwendung des symmetrischen Schlüssels umfaßt.

6. Verfahren nach Anspruch 4, ferner umfassend ein Verschlüsseln der Datenstruktur unter Verwendung des symmetrischen Schlüssels.

7. Verfahren nach Anspruch 1, ferner umfassend ein Speichern des öffentlichen Schlüssels des Schlüsseldienstes auf einem geschützten Herstellungssystem.

8. Verfahren nach Anspruch 1, wobei der pseudozufällige Wert für die Vorrichtung eindeutig ist.

9. Gegenstand, umfassend: ein erstes Speichermedium mit einer Vielzahl von maschinenlesbaren Anweisungen, wobei die Anweisungen beim Ausführen durch einen Prozessor folgendes bewirken:
Einrichten eines geschützten Onlineservers zur Unterstützung von Schlüsselabrufanfragen von Clientcomputersystemen;
Erzeugen eines Schlüsseldienst-Schlüsselpaars aus öffentlichem/geheimem Schlüssel in einer sicheren Schlüsselabrufverarbeitung;
Erzeugen eines pseudozufälligen Werts für eine Vorrichtung;
Erzeugen einer der Vorrichtung zugeordneten ver-

schlüsselten Datenstruktur, wobei die verschlüsselte Datenstruktur einen geheimen Schlüssel umfaßt;
Erzeugen einer Kennung für die verschlüsselte Datenstruktur basierend auf dem pseudozufälligen Wert;
Speichern der Kennung und der verschlüsselten Datenstruktur auf dem geschützten Onlineserver; und
Speichern des pseudozufälligen Werts und eines Hash-Werts des öffentlichen Schlüssels des Schlüsseldiensts in einen nicht-flüchtigen Speicher in der Vorrichtung.

10. Gegenstand nach Anspruch 9, ferner umfassend Anweisungen zum Erzeugen eines Schlüsselpaars der Direktnachweisfamilie für eine Vorrichtungsklasse.

11. Gegenstand nach Anspruch 10, wobei der geheime Schlüssel einen einem öffentlichen Schlüssel des Schlüsselpaars der Direktnachweisfamilie zugeordneten geheimen Direktnachweisschlüssel umfaßt, und ferner umfassend Anweisungen zum Hashen des geheimen Direktnachweisschlüssels zum Erzeugen des Extrakts des geheimen Schlüssels.

12. Gegenstand nach Anspruch 9, ferner umfassend Anweisungen zum Erzeugen eines symmetrischen Schlüssels basierend auf dem pseudozufälligen Wert für die Vorrichtung.

13. Gegenstand nach Anspruch 12, wobei die Anweisungen zum Erzeugen der Kennung Anweisungen zum Verschlüsseln eines Datenwerts unter Verwendung des symmetrischen Schlüssels umfassen.

14. Gegenstand nach Anspruch 12, ferner umfassend Anweisungen zum Verschlüsseln der Datenstruktur unter Verwendung des symmetrischen Schlüssels.

15. Gegenstand nach Anspruch 9, ferner umfassend Anweisungen zum Speichern des öffentlichen Schlüssels des Schlüsseldienstes auf einem geschützten Herstellungssystem.

16. Gegenstand nach Anspruch 9, wobei der pseudozufällige Wert für die Vorrichtung eindeutig ist.

17. Verfahren, umfassend:
Bestimmen, ob eine verschlüsselte Datenstruktur, die einen geheimen Schlüssel umfaßt und einer in einem Computersystem installierten Vorrichtung zugeordnet ist, in einem Speicher in dem Computersystem gespeichert ist; und
wenn die verschlüsselte Datenstruktur nicht gespeichert ist, Erhalten der der Vorrichtung zugeordneten verschlüsselten Datenstruktur von einem geschützten Onlineserver, auf den durch das Computersystem zugegriffen werden kann, wobei der Server eine Datenbank verschlüsselter Datenstrukturen speichert.

18. Verfahren nach Anspruch 17, wobei das Erhalten der verschlüsselten Datenstruktur ein Ausgeben eines Schlüssel-Erhalten-Befehls an die Vorrichtung umfaßt, um einen Prozess zum Erhalten des geheimen Schlüssels zu initiieren.

19. Verfahren nach Anspruch 17, wobei der geheime Schlüssel einen einem öffentlichen Schlüssel des Schlüsselpaars der Direktnachweisfamilie für eine Vorrichtungsklasse zugeordneten geheimen Direktnachweisschlüssel umfaßt.

20. Verfahren nach Anspruch 18, wobei der Prozess zum Erhalten des geheimen Schlüssels ein Erhalten eines öffentlichen Schlüssels des Schlüsseldienstes, der durch einen entsprechenden geheimen Schlüssel des Schlüsseldienstes unterschrieben ist, durch die Vorrichtung von dem geschützten Onlineserver umfaßt.

21. Verfahren nach Anspruch 20, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Erzeugen eines symmetrischen Schlüssels auf der Basis eines in der Vorrichtung gespeicherten eindeutigen pseudozufälligen Werts und einer Vorrichtungskennung auf der Basis des pseudozufälligen Werts für die verschlüsselte Datenstruktur umfaßt.

22. Verfahren nach Anspruch 21, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Erzeugen eines transienten symmetrischen Schlüssels durch die Vorrichtung, einen Aufbau einer Nachricht zum Abrufen des Schlüssels, welche die Vorrichtungskennung und den transienten symmetrischen Schlüssel enthält, ein Verschlüsseln der Nachricht zum Abrufen des Schlüssels unter Verwendung des öffentlichen Schlüssels des Schlüsseldienstes und ein Senden der verschlüsselten Nachricht zum Abrufen des Schlüssels an den geschützten Onlineserver umfaßt.

23. Verfahren nach Anspruch 22, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Entschlüsseln der verschlüsselten Nachricht zum Abrufen des Schlüssels unter Verwendung des geheimen Schlüssels des Schlüsseldienstes zum Erhalten der Vorrichtungskennung umfaßt.

24. Verfahren nach Anspruch 23, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Durchsuchen des geschützten Onlineservers auf einen Eintrag verschlüsselter Datenstrukturen in der Datenbank, welche durch eine der erzeugten Vorrichtungskennung entsprechenden Kennung angezeigt werden, ein Aufbauen einer Nachricht zum Beantworten des Schlüssels, die die verschlüsselte Datenstruktur in dem Eintrag enthält, ein Verschlüsseln der

Nachricht zum Beantworten des Schlüssels mit dem transienten symmetrischen Schlüssel, und ein Übertragen der Nachricht zum Beantworten des Schlüssels an die Vorrichtung umfaßt.

25. Verfahren nach Anspruch 24, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Entschlüsseln durch die Vorrichtung der verschlüsselten Nachricht zum Beantworten des Schlüssels unter Verwendung des transienten symmetrischen Schlüssels zum Erhalten der verschlüsselten Datenstruktur umfaßt.

26. Verfahren nach Anspruch 25, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Entschlüsseln der von dem geschützten Onlineserver erhaltenen verschlüsselten Datenstruktur unter Verwendung des symmetrischen Schlüssels zum Erhalten des geheimen Schlüssels und des Extrakts des geheimen Schlüssels umfaßt.

27. Verfahren nach Anspruch 25, wobei der Prozess zum Erhalten des geheimen Schlüssels ferner ein Hashen des geheimen Schlüssels zum Erzeugen eines neuen Extrakts des geheimen Schlüssels, ein Vergleichen des Extrakts des geheimen Schlüssels von der entschlüsselten Datenstruktur mit dem neuen Extrakt des geheimen Schlüssels und ein Annehmen des geheimen Schlüssels als für die Vorrichtung gültig, wenn die Extrakte übereinstimmen, umfaßt.

28. Gegenstand, umfassend: ein Speichermedium mit einer Vielzahl maschinenlesbarer Anweisungen, wobei die Anweisungen beim Ausführen durch einen Prozessor das Erhalten eines geheimen Schlüssels für eine in einem Computersystem installierte Vorrichtung bewirken durch
Bestimmen, ob eine verschlüsselte Datenstruktur, die einen geheimen Schlüssel umfaßt und einer in einem Computersystem installierten Vorrichtung zugeordnet ist, in einem Speicher in dem Computersystem gespeichert ist; und
wenn die verschlüsselte Datenstruktur nicht gespeichert ist, Erhalten der der Vorrichtung zugeordneten verschlüsselten Datenstruktur von einem geschützten Onlineserver, auf den durch das Computersystem zugegriffen werden kann, wobei der Server eine Datenbank verschlüsselter Datenstrukturen speichert.

29. Gegenstand nach Anspruch 28, wobei die Anweisungen zum Erhalten der verschlüsselten Datenstruktur Anweisungen zum Ausgeben des Befehls zum Erhalten des Schlüssels an die Vorrichtung zum Initiieren eines Prozesses zum Erhalten eines geheimen Schlüssels umfassen.

30. Gegenstand nach Anspruch 28, wobei der geheime Schlüssel einen einem öffentlichen Schlüssel eines Schlüsselpaars einer Direktnachweisgruppe für eine Vorrichtungsklasse zugeordneten geheimen Direktnachweisschlüssel umfaßt.

31. Gegenstand nach Anspruch 29, wobei Anweisungen für den Prozess zum Erhalten des geheimen Schlüssels Anweisungen zum Erhalten einen öffentlichen Schlüssel des Schlüsseldienstes durch die Vorrichtung von dem geschützten Onlineserver umfassen, die durch einen entsprechenden geheimen Schlüssel des Schlüsseldienstes unterzeichnet sind.

32. Gegenstand nach Anspruch 31, wobei Anweisungen für den Prozess zum Erhalten des geheimen Schlüssels ferner Anweisungen zum Erzeugen eines symmetrischen Schlüssels auf der Basis eines in der Vorrichtung gespeicherten eindeutigen pseudozufälligen Werts und einer Vorrichtungskennung, die auf dem pseudozufälligen Wert basiert, für die verschlüsselte Datenstruktur umfassen.

33. Gegenstand nach Anspruch 32, wobei Anweisungen für den Prozess zum Erhalten des geheimen Schlüssels ferner Anweisungen zu einem Erzeugen eines transienten symmetrischen Schlüssels durch die Vorrichtung, zu einem Aufbauen einer Nachricht zum Abrufen des Schlüssels, welche die Vorrichtungskennung und den transienten symmetrischen Schlüssel enthält, zu einem Verschlüsseln der Nachricht zum Abrufen des Schlüssels unter Verwendung des öffentlichen Schlüssels des Schlüsseldienstes und zu einem Senden der verschlüsselten Nachricht zum Abrufen des Schlüssels an den geschützten Onlineserver umfaßt.

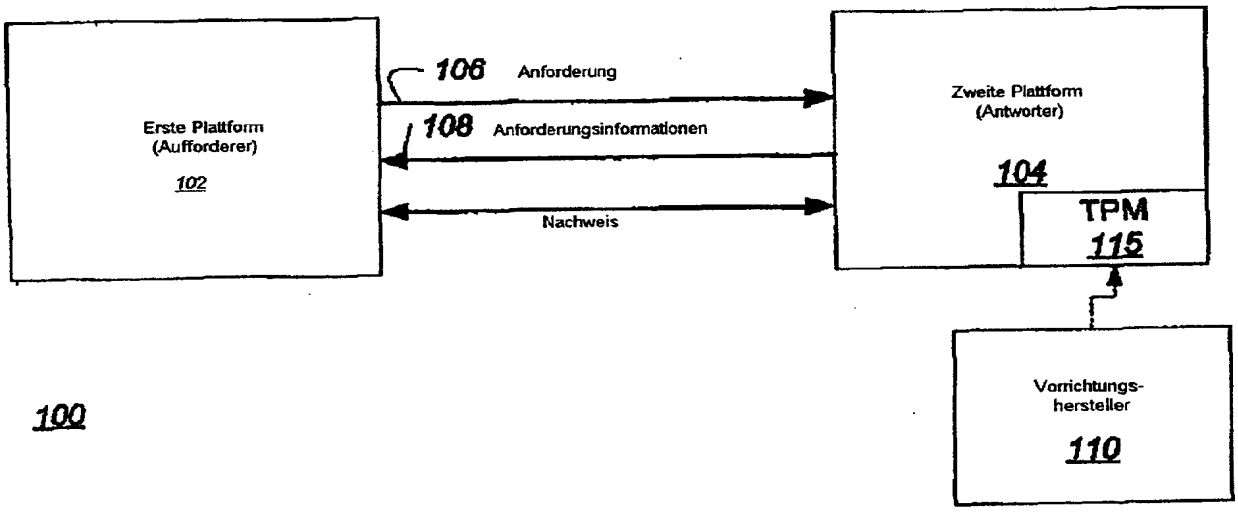
34. System zum Liefern eines geheimen Schlüssels an eine in einem Clientcomputersystem gespeicherte Vorrichtung unter Verwendung eines sicheren Protokolls, das folgendes umfaßt:
einen geschützten Onlineserver, der für das Clientcomputersystem zugänglich ist und zum Erzeugen eines Schlüsselpaars aus öffentlichem/geheimem Schlüssel, zum Speichern einer Datenbank verschlüsselter Datenstrukturen, wobei jede verschlüsselte Datenstruktur einen einer ausgewählten Vorrichtung entsprechenden geheimen Schlüssel enthält, und zum sicheren Kommunizieren einer ausgewählten verschlüsselten Datenstruktur an die Vorrichtung konfiguriert ist;
ein geschütztes System, das mit dem geschützten Server gekoppelt und dazu konfiguriert ist, die der Vorrichtung zugeordnete verschlüsselte Datenstruktur zu erzeugen, den öffentlichen Schlüssel des Schlüsseldienstes von dem geschützten Server zu empfangen und die verschlüsselte Datenstruktur an den geschützten Onlineserver zu senden; und ein Produktionssystem, das mit dem geschützten System gekoppelt und dazu konfiguriert ist, einen Hash-Wert des öffentlichen Schlüssels des Schlüsseldienstes und einen eindeutigen pseudozufälligen Wert von dem geschützten System zu empfangen

und vor der Installation der Vorrichtung in ein Clientcomputersystem den Hash-Wert des öffentlichen Schlüssels des Schlüsseldienstes und den eindeutigen pseudozufälligen Wert in einen nicht-flüchtigen Speicher der Vorrichtung zu speichern.

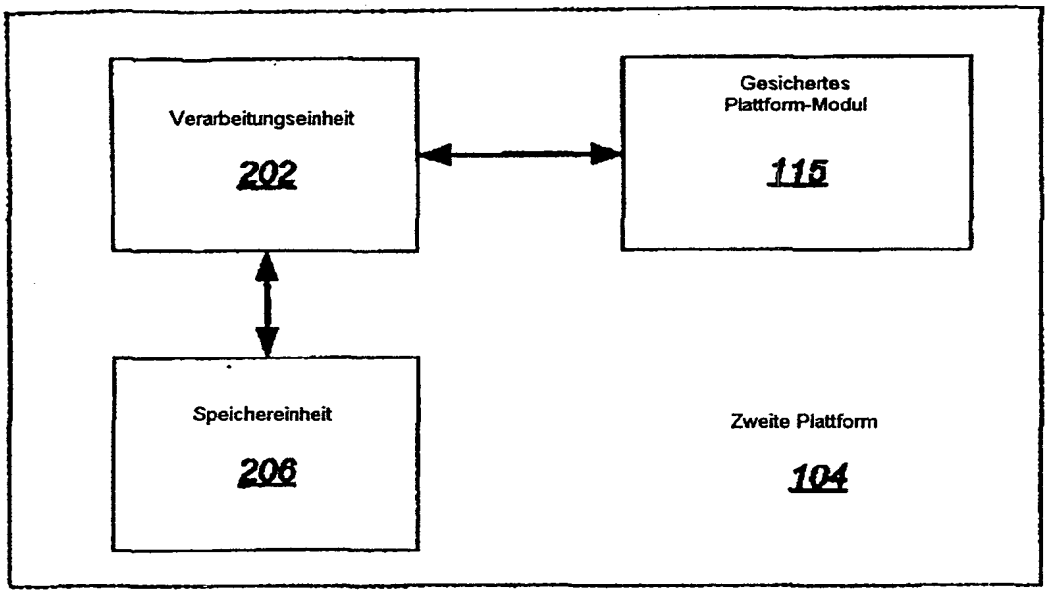
35. System nach Anspruch 34, wobei der geheime Schlüssel einen einem öffentlichen Schlüssel des Schlüsselpaars der Direktnachweisfamilie zugeordneten geheimen Direktnachweisschlüssel umfaßt.

Es folgen 12 Blatt Zeichnungen

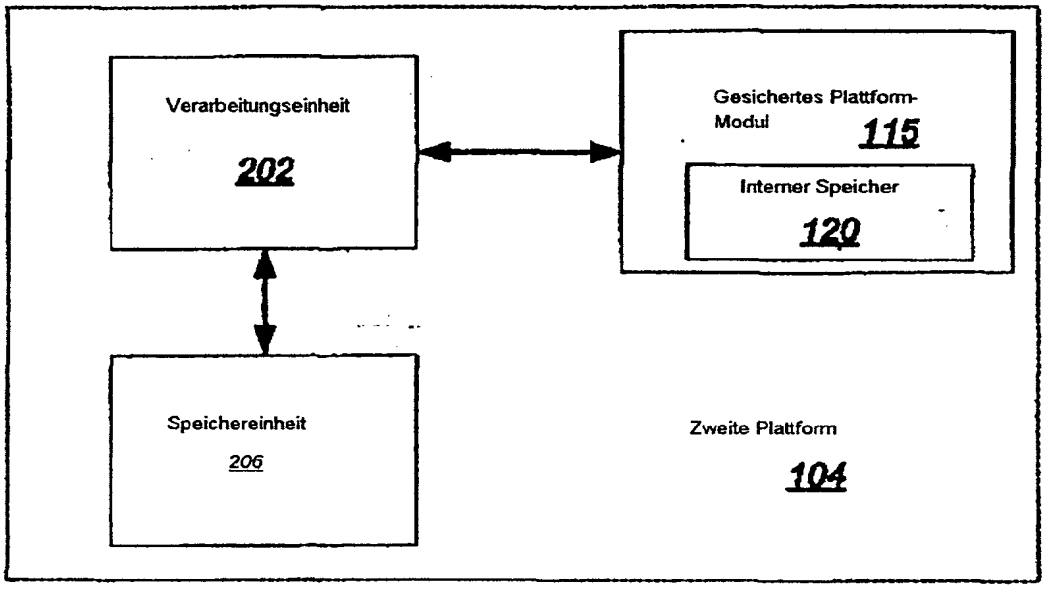
Anhängende Zeichnungen



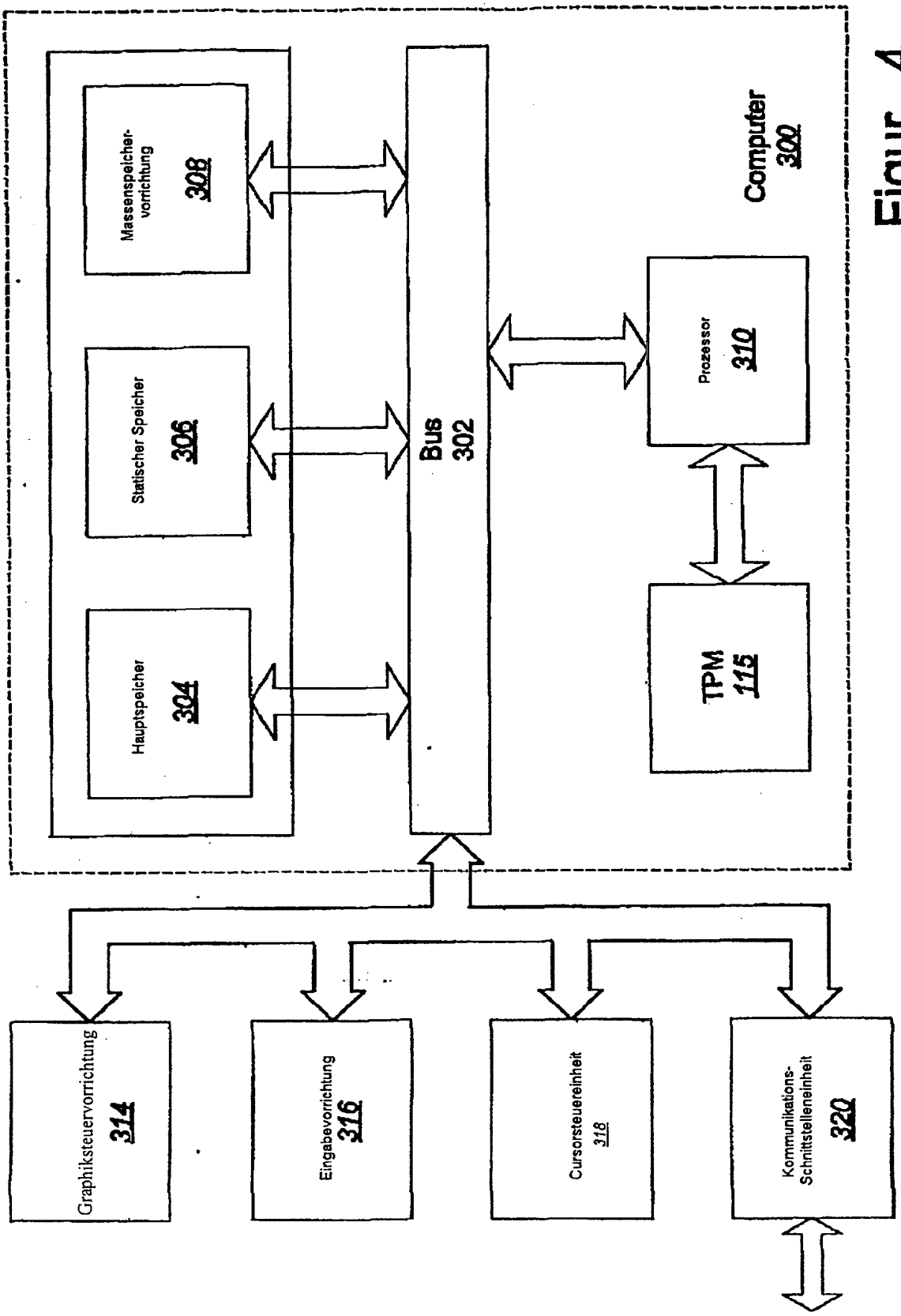
Figur 1



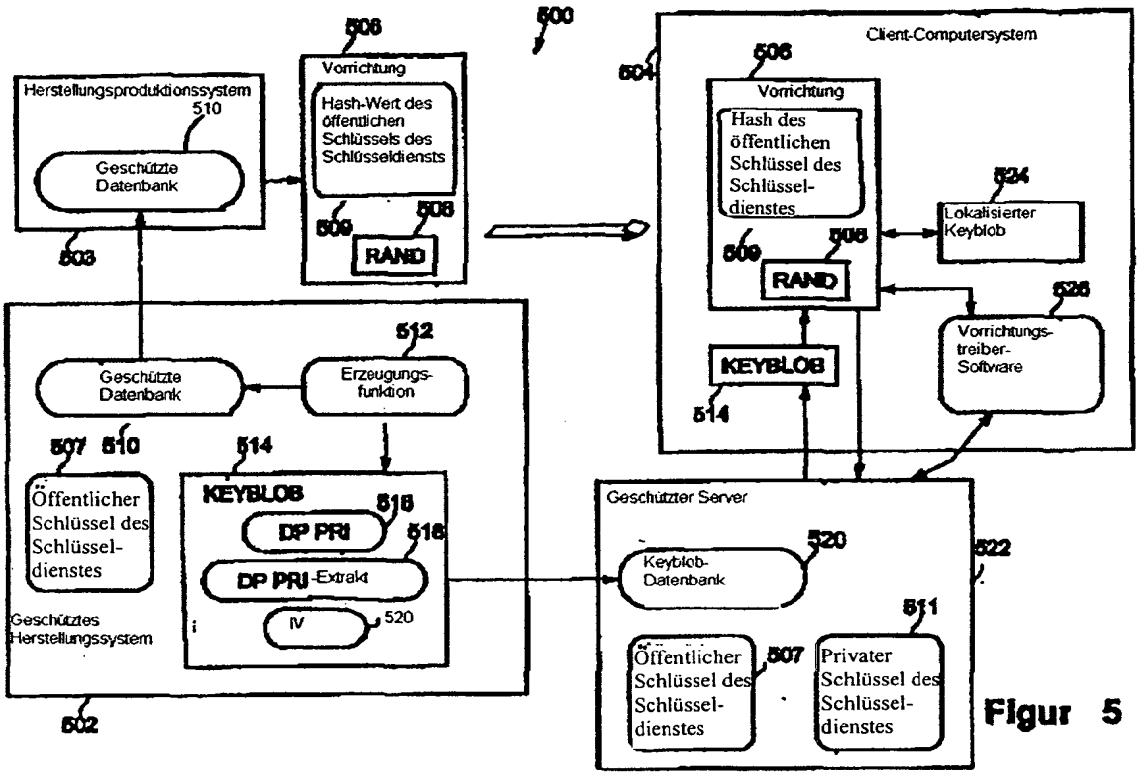
Figur 2



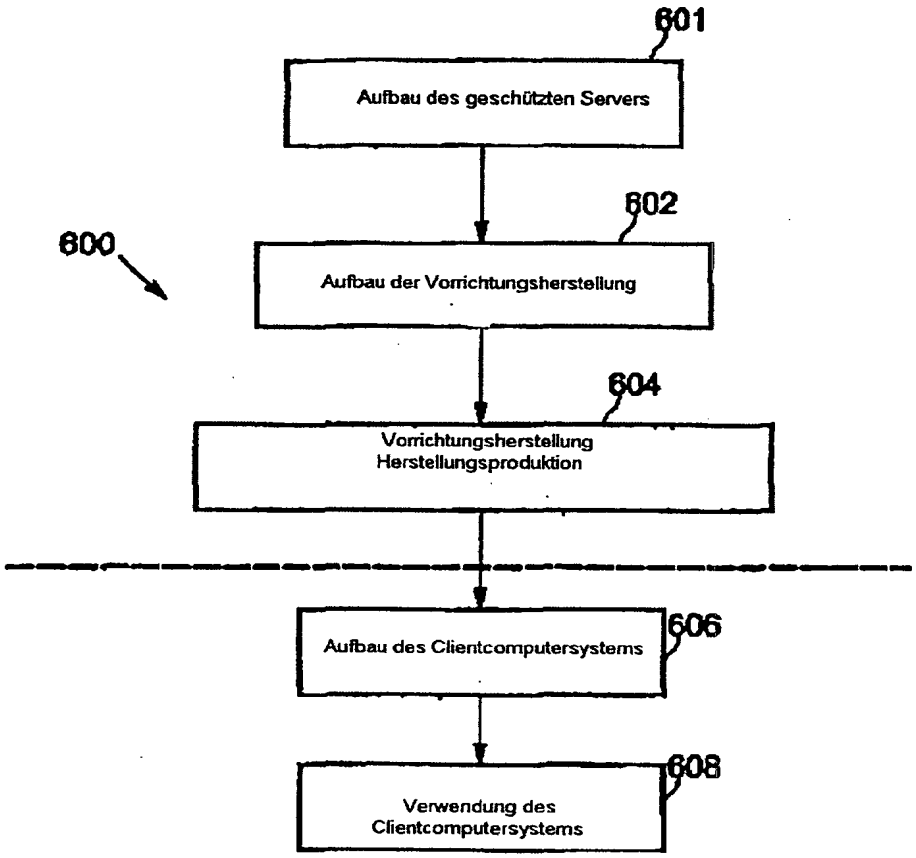
Figur 3


Computer
300
Massenspeicher-vorrichtung
308
Statischer Speicher
306
Hauptspeicher
304
Bus
302
Prozessor
310
TPM
115
104
Graphiksteuervorrichtung
314
Eingabevorrichtung
316
Cursorsteuereinheit
318
Kommunikations-Schnittstelleneinheit
320

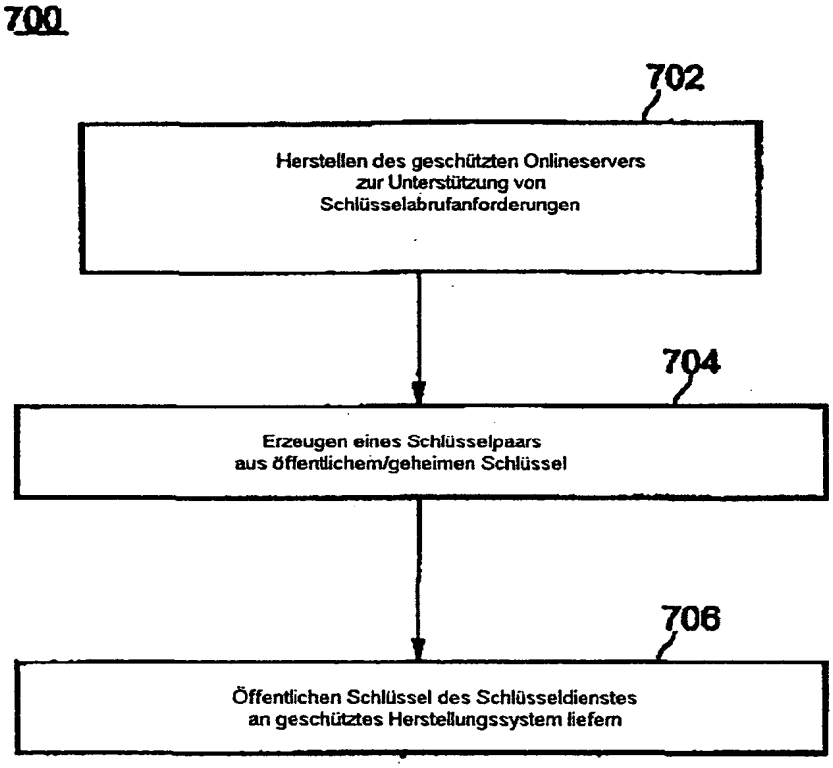
Figur 4


500
Herstellungsproduktionssystem
510
Geschützte Datenbank
503
506
Vorrichtung
Hash-Wert des öffentlichen Schlüssels des Schlüsseldiensts
509
508
RAND
Client-Computersystem
504
506
Vorrichtung
Hash des öffentlichen Schlüssel des Schlüssel-dienstes
524
Lokalisierter Keyblob
509
508
RAND
526
Vorrichtungs-treiber-Software
KEYBLOB
514
512
Geschützte Datenbank
Erzeugungs-funktion
507
510
Öffentlicher Schlüssel des Schlüssel-dienstes
514
KEYBLOB
516
DP PRI
516
DP PRI-Extrakt
IV
520
Geschütztes Herstellungssystem
502
Geschützter Server
520
Keyblob-Datenbank
522
511
Öffentlicher Schlüssel des Schlüssel-dienstes
507
Privater Schlüssel des Schlüssel-dienstes

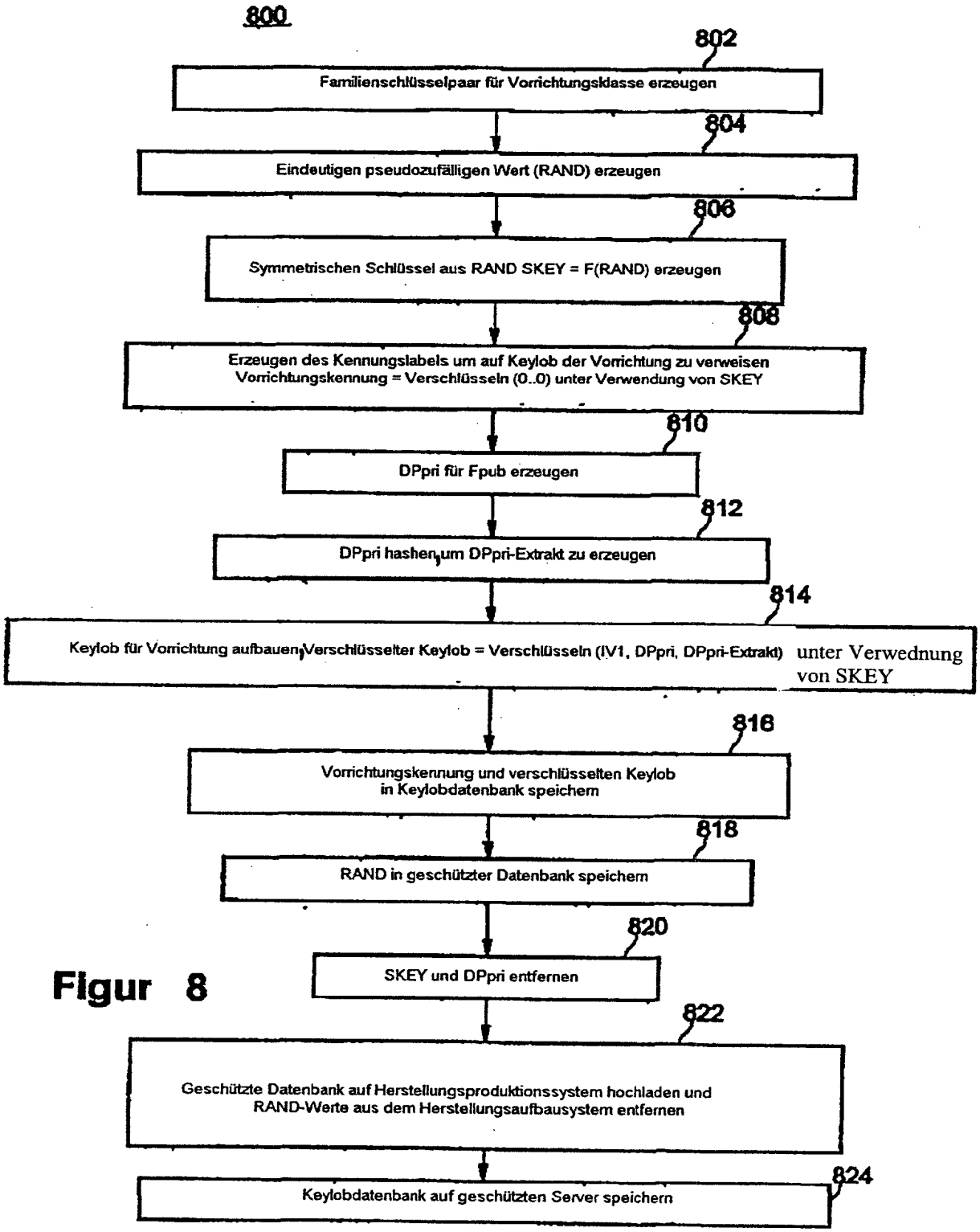
Figur 5


601
Aufbau des geschützten Servers
602
600
Aufbau der Vorrichtungsherstellung
604
Vorrichtungsherstellung
Herstellungsproduktion
606
Aufbau des Clientcomputersystems
608
Verwendung des
Clientcomputersystems

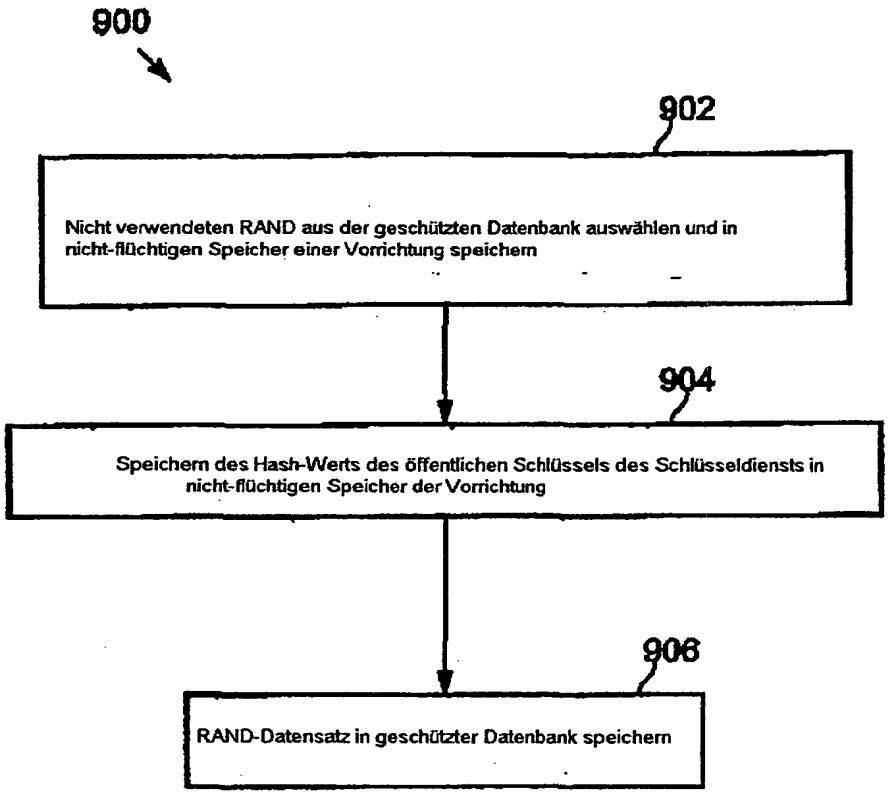
Figur 6


700
702
Herstellen des geschützten Onlineservers zur Unterstützung von Schlüsselabrufanforderungen
704
Erzeugen eines Schlüsselpaars aus öffentlichem/geheimen Schlüssel
706
Öffentlichen Schlüssel des Schlüsseldienstes an geschütztes Herstellungssystem liefern

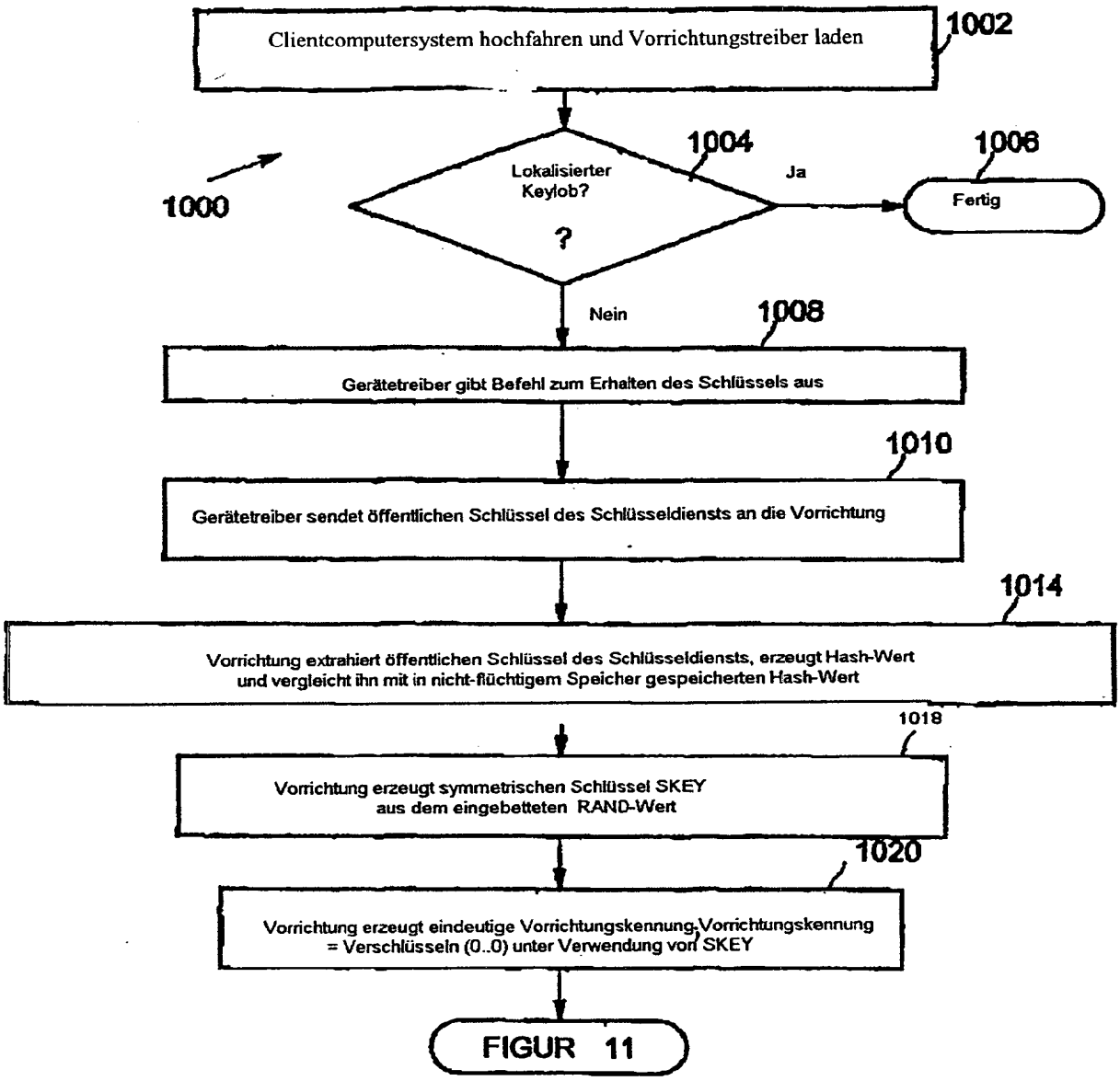
Figur 7


800
802
Familienschlüsselpaar für Vorrichtungsklasse erzeugen
804
Eindeutigen pseudozufälligen Wert (RAND) erzeugen
806
Symmetrischen Schlüssel aus RAND SKEY = F(RAND) erzeugen
808
Erzeugen des Kennungslabels um auf Keylob der Vorrichtung zu verweisen
Vorrichtungskennung = Verschlüsseln (0..0) unter Verwendung von SKEY
810
DPpri für Fpub erzeugen
812
DPpri hashen, um DPpri-Extrakt zu erzeugen
814
Keylob für Vorrichtung aufbauen, Verschlüsselter Keylob = Verschlüsseln (IV1, DPpri, DPpri-Extrakt) unter Verwednung von SKEY
816
Vorrichtungskennung und verschlüsselten Keylob in Keylobdatenbank speichern
818
RAND in geschützter Datenbank speichern
820
SKEY und DPpri entfernen
822
Geschützte Datenbank auf Herstellungsproduktionssystem hochladen und RAND-Werte aus dem Herstellungsaufbausystem entfernen
824
Keylobdatenbank auf geschützten Server speichern

Figur 8

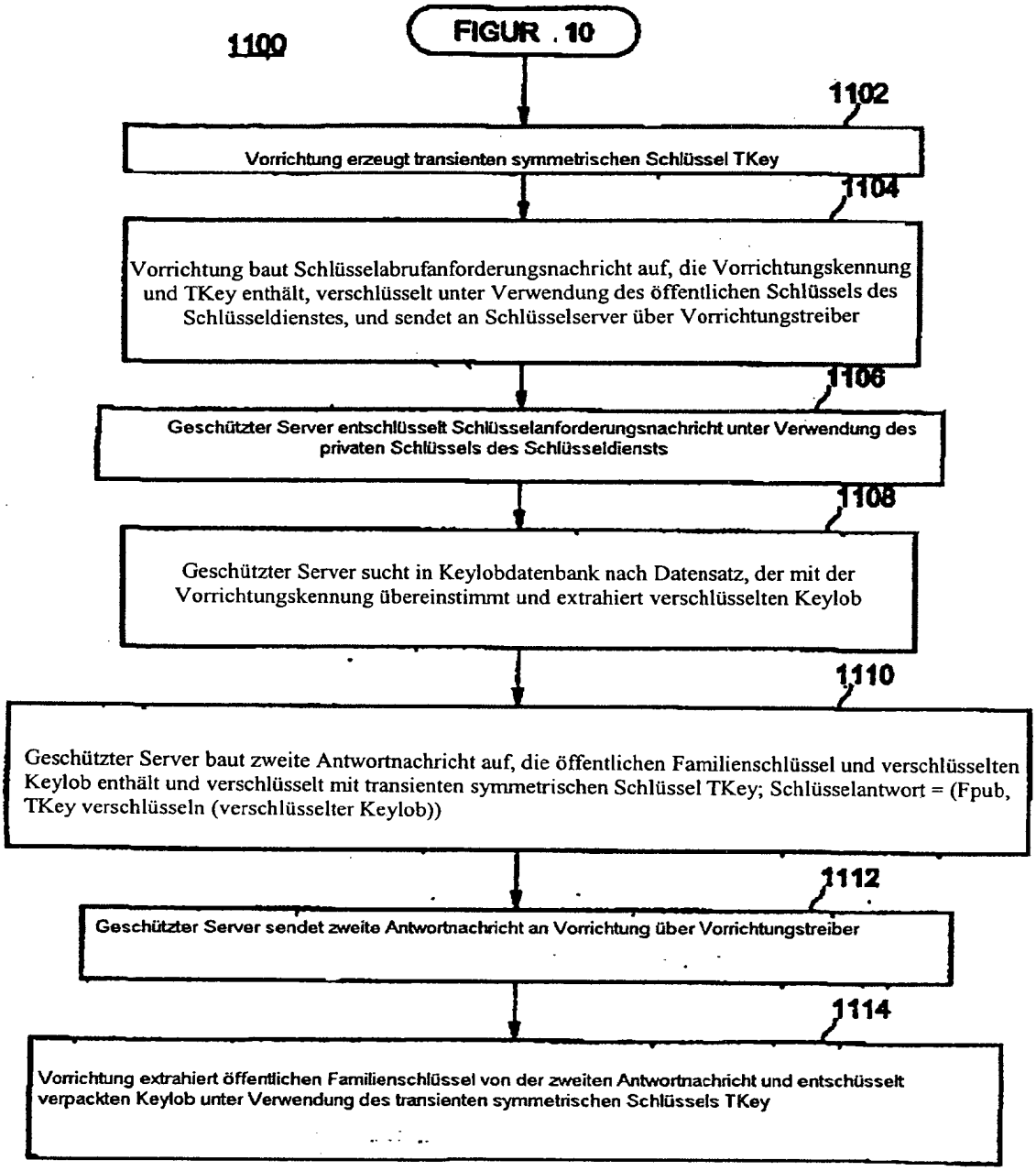

900
902
Nicht verwendeten RAND aus der geschützten Datenbank auswählen und in nicht-flüchtigen Speicher einer Vorrichtung speichern
904
Speichern des Hash-Werts des öffentlichen Schlüssels des Schlüsseldiensts in nicht-flüchtigen Speicher der Vorrichtung
906
RAND-Datensatz in geschützter Datenbank speichern

Figur 9



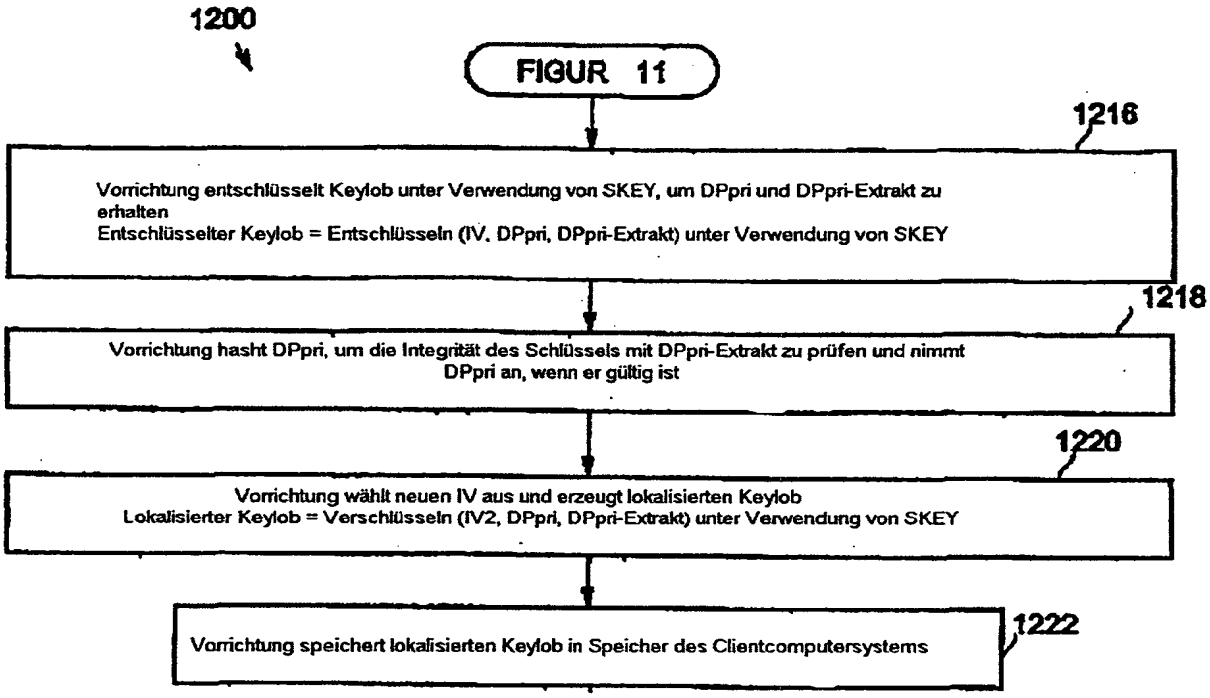
FIGUR 11

Figur 10

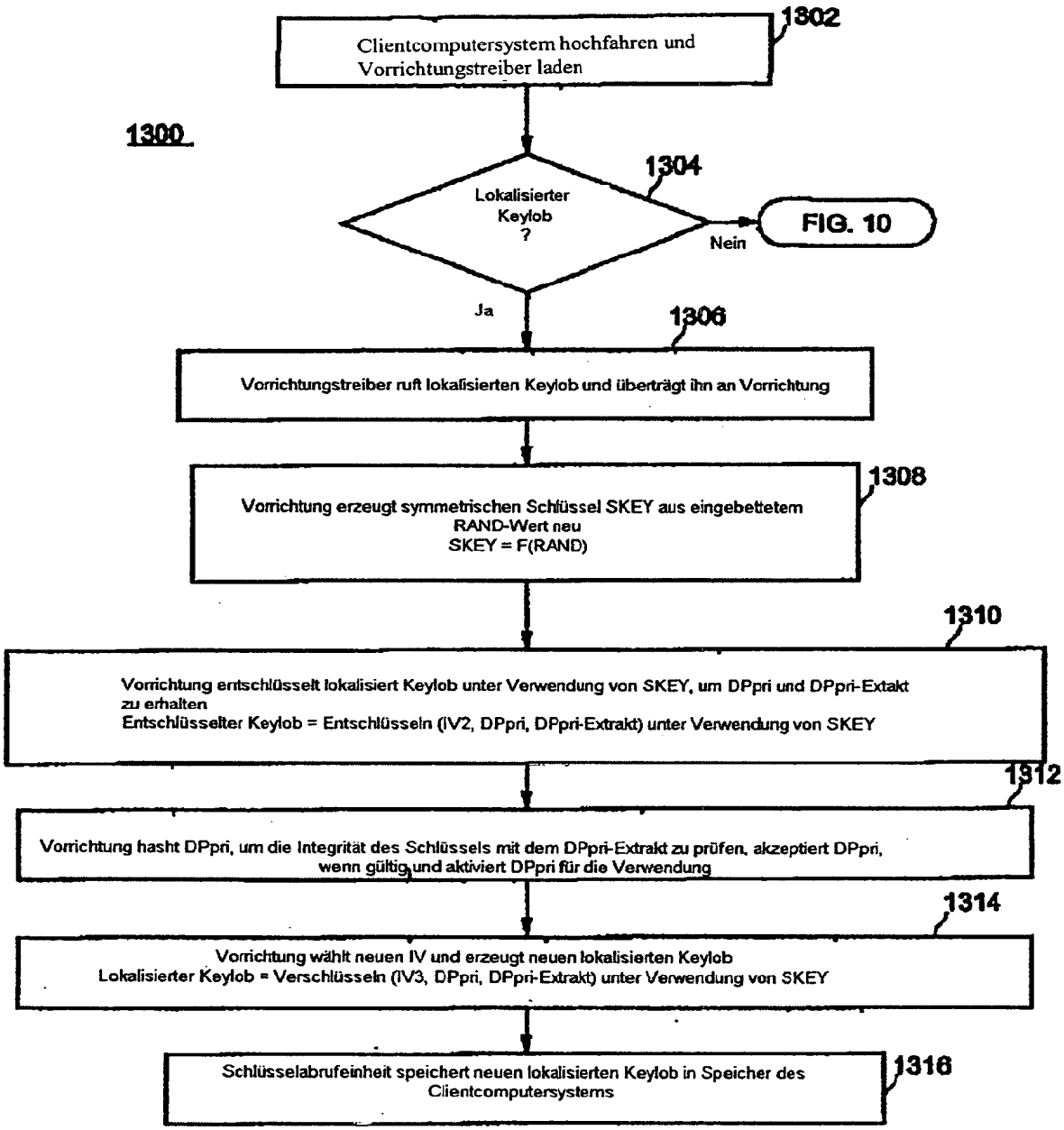


FIGUR 11

FIGUR . 12


1200
FIGUR 11
1216
Vorrichtung entschlüsselt Keylob unter Verwendung von SKEY, um DPpri und DPpri-Extrakt zu erhalten
Entschlüsselter Keylob = Entschlüsseln (IV, DPpri, DPpri-Extrakt) unter Verwendung von SKEY
1218
Vorrichtung hasht DPpri, um die Integrität des Schlüssels mit DPpri-Extrakt zu prüfen und nimmt DPpri an, wenn er gültig ist
1220
Vorrichtung wählt neuen IV aus und erzeugt lokalisierten Keylob
Lokalisierter Keylob = Verschlüsseln (IV2, DPpri, DPpri-Extrakt) unter Verwendung von SKEY
1222
Vorrichtung speichert lokalisierten Keylob in Speicher des Clientcomputersystems

Figur 12


1300
1302
Clientcomputersystem hochfahren und Vorrichtungstreiber laden
1304
Lokalisierter Keylob ?
Nein
FIG. 10
Ja
1306
Vorrichtungstreiber ruft lokalisierten Keylob und überträgt ihn an Vorrichtung
1308
Vorrichtung erzeugt symmetrischen Schlüssel SKEY aus eingebettetem RAND-Wert neu
SKEY = F(RAND)
1310
Vorrichtung entschlüsselt lokalisiert Keylob unter Verwendung von SKEY, um DPpri und DPpri-Extakt zu erhalten
Entschlüsselter Keylob = Entschlüsseln (IV2, DPpri, DPpri-Extrakt) unter Verwendung von SKEY
1312
Vorrichtung hasht DPpri, um die Integrität des Schlüssels mit dem DPpri-Extrakt zu prüfen, akzeptiert DPpri, wenn gültig und aktiviert DPpri für die Verwendung
1314
Vorrichtung wählt neuen IV und erzeugt neuen lokalisierten Keylob
Lokalisierter Keylob = Verschlüsseln (IV3, DPpri, DPpri-Extrakt) unter Verwendung von SKEY
1316
Schlüsselabrufeinheit speichert neuen lokalisierten Keylob in Speicher des Clientcomputersystems

Figur 13